

Produkthandbuch

Revision A

McAfee Advanced Threat Defense 3.4.2

COPYRIGHT

Copyright © 2014 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

MARKEN

Intel und das Intel-Logo sind eingetragene Marken der Intel Corporation in den USA und/oder anderen Ländern. McAfee und das McAfee-Logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource und VirusScan sind eingetragene Marken oder Marken von McAfee, Inc. oder seinen Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer.

LIZENZINFORMATIONEN

LIZENZVEREINBARUNG

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DEN BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWARE-PAKET ODER SEPARAT (ALS BROSCHÜRE, DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE AUF DER WEBSEITE VERFÜGBAR IST, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN McAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

Inhaltsverzeichnis

Einleitung **9**

Informationen zu diesem Handbuch 9
Zielgruppe 9
Konventionen 9
Quellen für Produktinformationen 10

1 Malware-Erkennung und McAfee® Advanced Threat Defense **11**

Das Malware-Bedrohungsszenario 11
Die McAfee Advanced Threat Defense-Lösung 12
McAfee Advanced Threat Defense-Bereitstellungsoptionen 14
Vorteile von McAfee Advanced Threat Defense 17

2 Einrichten der McAfee Advanced Threat Defense Appliance **19**

Über die McAfee Advanced Threat Defense-Appliance 19
Funktionen einer McAfee Advanced Threat Defense-Appliance 19
Vor dem Installieren der McAfee Advanced Threat Defense Appliance 20
Warnungen und Hinweise 21
Nutzungsbeschränkungen 21
Auspacken der Lieferung 22
Überprüfen der Lieferung 22
Hardware-Spezifikationen und Umgebungsanforderungen 25
Portnummern 27
Einrichten der McAfee Advanced Threat Defense 27
Montieren und Entfernen von Rackgriffen 28
Installieren oder Entfernen der Appliance aus dem Rack 28
Einschalten der McAfee Advanced Threat Defense Appliance 30
Umgang mit der Frontblende 30
Verbinden des Netzwerkkabels 31
Konfigurieren der Netzwerkinformationen für die McAfee Advanced Threat Defense Appliance 31

3 Zugreifen auf die McAfee Advanced Threat Defense-Web-Anwendung **35**

McAfee Advanced Threat Defense-Client-Anforderungen 35
Zugreifen auf die McAfee Advanced Threat Defense-Web-Anwendung 36

4 Verwalten von Advanced Threat Defense **37**

Verwalten von McAfee Advanced Threat Defense-Benutzern 37
Anzeigen von Benutzerprofilen 38
Hinzufügen von Benutzern 40
Bearbeiten von Benutzern 43
Löschen von Benutzern 44
Überwachen der McAfee Advanced Threat Defense-Leistung 44
Upgrade von McAfee Advanced Threat Defense und Android-VM 44
Upgrade der McAfee Advanced Threat Defense-Software von 3.0.2.xx auf 3.0.4.xx 45
Upgrade der McAfee Advanced Threat Defense-Software von 3.0.2.36 auf 3.2.0.xx 48

Upgrade der McAfee Advanced Threat Defense-Software von 3.0.4.xx auf 3.2.0.xx 51
Upgrade der ATD-Software von 3.2.0.xx auf 3.2.2.xx 53
Upgrade der Android-Analyse-VM 55
Fehlerbehebung 58
Exportieren von McAfee Advanced Threat Defense-Protokollen 59
Neuerstellen der Analyse-VMs 60
Löschen der Analyseergebnisse 61
Sichern und Wiederherstellen der Advanced Threat Defense-Datenbank 61
Planen einer Datenbanksicherung 62
Wiederherstellen einer Datenbanksicherung – Spezifische Sicherungsdatei und vorhergehende Sicherungsdatei 65

5 Erstellen einer Analyse-VM 71
Erstellen einer VMDK-Datei für Windows XP 73
Erstellen einer VMDK-Datei für Windows 2003 Server 105
Erstellen einer VMDK-Datei für Windows 7 137
Erstellen einer VMDK-Datei für Windows 2008 Server 163
Erstellen einer VMDK-Datei für Windows 8 188
Importieren einer VMDK-Datei in McAfee Advanced Threat Defense 230
Konvertieren der VMDK-Datei in eine Image-Datei 230
Verwalten von VM-Profilen 233
Anzeigen von VM-Profilen 234
Erstellen von VM-Profilen 234
Bearbeiten von VM-Profilen 240
Löschen von VM-Profilen 241
Anzeigen des VM-Erstellungsprotokolls 241

6 Konfigurieren von McAfee Advanced Threat Defense für die Malware-Analyse 243
Begriffe 243
Grundlegende Schritte zum Konfigurieren der Malware-Analyse 247
Wie analysiert McAfee Advanced Threat Defense Malware? 248
Internetzugriff für Probedateien 248
Verwalten von Analyseprofilen 251
Anzeigen der Analyseprofile 252
Erstellen von Analyseprofilen 253
Bearbeiten von Analyseprofilen 256
Löschen von Analyseprofilen 256
Integration in McAfee ePO 256
Konfigurieren der McAfee ePO-Integration 258
Integration in Data Exchange Layer 259
Konfigurieren der Data Exchange Layer-Integration 260
Integration in McAfee Next Generation Firewall 261
Konfigurieren des Proxy-Servers für die Internetverbindung 261
Angeben von Proxy-Einstellungen für den Datenverkehr von Global Threat Intelligence 262
Festlegen der Malware-Website-Proxy-Einstellungen für Malware-Datenverkehr 263
Konfigurieren der Syslog-Einstellung 264
Konfigurieren von DNS-Einstellungen 267
Konfigurieren der Datums- und Uhrzeiteinstellungen 267
Definieren von benutzerdefinierten YARA-Regeln zur Malware-Identifizierung 271
Erstellen der benutzerdefinierten YARA-Regeldatei 274
Importieren der benutzerdefinierten YARA-Regeldatei 277
Aktivieren oder Deaktivieren von YARA-Regeln 278
Ändern benutzerdefinierter YARA-Regeln 278

7 Analysieren von Malware 279
Analysieren von Dateien 279

Hochladen von Dateien zur Analyse mittels McAfee Advanced Threat Defense-Web-Anwendung . . . 280
Hochladen von Dateien zur Analyse über SFTP . . . 286
Analysieren von URLs . . . 287
Wie analysiert Advanced Threat Defense URLs? . . . 287
Hochladen von URLs zur Analyse mittels Advanced Threat Defense-Web-Anwendung . . . 288
Konfigurieren der Seite "Analysis Status" (Analysestatus) . . . 290
Anzeigen der Analyseergebnisse . . . 294
Anzeigen des Berichts "Analysis Summary" (Analyseübersicht) . . . 297
Bericht zu betroffenen Dateien . . . 304
Disassembly-Ergebnisse . . . 304
Bericht "Logic Path Graph" (Logisches Pfaddiagramm) . . . 305
User API-Protokoll . . . 310
Herunterladen der vollständigen Ergebnisse als ZIP-Datei . . . 310
Download der Originalprobe . . . 312
Arbeiten mit dem McAfee Advanced Threat Defense-Dashboard . . . 312
Malware-Analysemonitore . . . 313
Monitor "VM Creation Status" . . . 317
McAfee Advanced Threat Defense-Leistungsmonitore . . . 317

8 Clustering von McAfee Advanced Threat Defense Appliances 321
Erläuterungen zum McAfee Advanced Threat Defense-Cluster . . . 321
Voraussetzungen und Anmerkungen . . . 322
Netzwerkverbindungen für ein Advanced Threat Defense-Cluster . . . 323
Funktionsweise des Advanced Threat Defense-Clusters . . . 325
Prozessablauf für Network Security Platform . . . 329
Prozessablauf für McAfee Web Gateway . . . 330
Konfigurieren eines Advanced Threat Defense-Clusters – Grundlegende Schritte . . . 331
Erstellen des McAfee Advanced Threat Defense-Clusters . . . 332
Überwachen des Status eines Advanced Threat Defense-Clusters . . . 337
Einsenden von Proben an ein Advanced Threat Defense-Cluster . . . 341
Überwachen des Analysestatus für ein Advanced Threat Defense-Cluster . . . 341
Überwachen von Analyseergebnissen für ein Advanced Threat Defense-Cluster . . . 342
Ändern der Konfigurationen für einMcAfee Advanced Threat Defense-Cluster . . . 343

9 CLI-Befehle für McAfee Advanced Threat Defense 345
Ausgabe von CLI-Befehlen . . . 345
Ausgeben eines Befehls über die Konsole . . . 345
Ausgeben eines Befehls über SSH . . . 346
Anmeldung bei der McAfee Advanced Threat Defense Appliance mittels SSH-Client . . . 346
Auto-Vervollständigung . . . 346
CLI-Syntax . . . 346
Obligatorische Befehle . . . 347
Anmelden über die Befehlszeilenschnittstelle (CLI) . . . 347
Bedeutung von "?" . . . 347
Verwalten der Festplatten der McAfee Advanced Threat Defense Appliance . . . 347
Liste der CLI-Befehle . . . 348
amas . . . 348
atdcounter . . . 348
backup reports . . . 348
backup reports date . . . 349
Blacklist . . . 349
clearstats . . . 350
cluster withdraw . . . 350
createDefaultVms . . . 350
db_repair . . . 351

deleteblacklist . . . 351
deletesamplereport . . . 351
diskcleanup . . . 351
dxlstatus . . . 351
docfilterstatus . . . 352
exit . . . 353
factorydefaults . . . 353
ftptest USER_NAME . . . 353
gti-restart . . . 353
help . . . 353
heuristic_analysis . . . 354
install msu . . . 357
lbstats . . . 357
list . . . 357
lowseveritystatus . . . 358
nslookup . . . 358
passwd . . . 358
ping . . . 359
quit . . . 359
reboot . . . 359
resetuiadminpasswd . . . 359
resetusertimeout . . . 360
restart network . . . 360
route add/delete network . . . 360
samplefilter . . . 360
set appliance dns A.B.C.D E.F.G.H WORD . . . 361
set intfport . . . 361
set intfport auto . . . 361
set intfport ip . . . 362
set intfport speed duplex . . . 362
set malware-intfport . . . 362
set mgmtport auto . . . 363
set mgmtport speed and duplex . . . 363
set filesizes . . . 363
set fips . . . 364
set ftp . . . 364
set heuristic_analysis . . . 365
set appliance gateway . . . 365
set appliance ip . . . 365
set appliance name . . . 365
set uilog . . . 366
set ui-timeout . . . 366
set waittime . . . 366
set whitelist . . . 367
show . . . 367
show epo-stats nsp . . . 367
show filesizes . . . 367
show fips . . . 368
show ftp . . . 368
show history . . . 368
show heuristic_analysis . . . 369
show intfport . . . 369
show msu . . . 369
show nsp scandetails . . . 369
show route . . . 370
show ui-timeout . . . 371

show uilog 371
show version 371
show waittime 371
shutdown 372
status 372
terminal 372
update_avdat 373
Vmlist 373
watchdog 373
set malware-intfport mgmt 373
whitelist 373

Index **375**

Einleitung

In diesem Handbuch finden Sie die erforderlichen Informationen für die Arbeit mit Ihrem McAfee-Produkt.

Inhalt

- *Informationen zu diesem Handbuch*
- *Quellen für Produktinformationen*

Informationen zu diesem Handbuch

In diesem Abschnitt werden die Zielgruppe des Handbuchs, die verwendeten typografischen Konventionen und Symbole sowie die Gliederung des Handbuchs beschrieben.

Zielgruppe

Die Dokumentation wurde von McAfee nach eingehender Recherche mit Blick auf die Zielgruppe verfasst.

Die Informationen in diesem Handbuch richten sich in erster Linie an:

- **Administratoren**: Personen, die für die Implementierung und Durchsetzung des Sicherheitsprogramms eines Unternehmens verantwortlich sind.
- **Benutzer**: Personen, die den Computer nutzen, auf dem die Software ausgeführt wird, und die auf einige oder alle Funktionen zugreifen können.

Konventionen

In diesem Handbuch werden folgende typografische Konventionen und Symbole verwendet.

Buchtitel, *Begriff*, *Hervorhebung*	Titel eines Buchs, Kapitels oder Themas; ein neuer Begriff; eine Hervorhebung.
Fett	Text, der stark hervorgehoben wird.
`Benutzereingabe, Code, Meldung`	Befehle oder andere Texte, die vom Benutzer eingegeben werden; ein Code-Beispiel; eine angezeigte Meldung.
Benutzeroberflächentext	Wörter aus der Benutzeroberfläche des Produkts, z. B. Optionen, Menüs, Schaltflächen und Dialogfelder.

Hypertext-Blau	Ein Link auf ein Thema oder eine externe Website.
	**Hinweis:** Zusätzliche Informationen, beispielsweise eine alternative Methode für den Zugriff auf eine Option.
	**Tipp:** Vorschläge und Empfehlungen.
	**Wichtig/Vorsicht:** Wichtige Ratschläge zum Schutz Ihres Computersystems, der Software-Installation, des Netzwerks, Ihres Unternehmens oder Ihrer Daten.
	**Warnung:** Wichtige Ratschläge, um körperliche Verletzungen bei der Nutzung eines Hardware-Produkts zu vermeiden.

Quellen für Produktinformationen

Nach der Veröffentlichung eines Produkts werden Informationen zu dem Produkt im Online-Knowledge Center von McAfee eingegeben.

Vorgehensweise

1. Rufen Sie McAfee ServicePortal unter http://support.mcafee.com auf und öffnen Sie die Registerkarte **Knowledge Center**.
2. Folgende Optionen stehen im Abschnitt **Support-Inhalte** zur Verfügung:
   - Klicken Sie auf **Produktdokumentation**, um Dokumentation für Produkte zu finden.
   - Klicken Sie auf **Technische Artikel**, um KnowledgeBase-Artikel aufzurufen.
3. Wählen Sie **Meine Filter nicht löschen** aus.
4. Geben Sie ein Produkt ein und wählen Sie die Version aus. Klicken Sie dann auf **Suchen**, um eine Liste der gewünschten Dokumente anzuzeigen.

1

Malware-Erkennung und McAfee® Advanced Threat Defense

Malware hat sich über die Jahre hinweg zu einem hochentwickelten Tool für bösartige Aktivitäten, darunter Diebstahl wertvoller Informationen, Zugriff auf Computerressourcen ohne Ihr Wissen und Störung des Geschäftsbetriebs, entwickelt. Gleichzeitig sorgt der technische Fortschritt dafür, dass unbeschränkte Möglichkeiten zur Verteilung bösartiger Dateien an ahnungslose Benutzer zur Verfügung stehen. Die Malware-Erkennung wird aufgrund der hunderttausend täglich auftretenden neuen Malware-Varianten zu einem immer komplexeren Unterfangen. Herkömmliche Malware-Schutztechniken reichen zum Schutz Ihres Netzwerks nicht mehr aus.

McAfees Antwort auf diese Herausforderung ist die McAfee Advanced Threat Defense-Lösung. Dabei handelt es sich um eine lokale Appliance, die die Erkennung und Vermeidung von Malware erleichtert. McAfee Advanced Threat Defense schützt sowohl vor bekannter Malware als auch vor Zero-Day-Bedrohungen und vor Malware, die bald nach dem Veröffentlichungsdatum einer Softwareversion in Umlauf gebracht wird. Die Dienstqualität für die Benutzer Ihres Netzwerks wird dabei nicht beeinträchtigt.

Von zusätzlichem Vorteil ist, dass McAfee Advanced Threat Defense eine integrierte Lösung ist. Neben den mehrschichtig angelegten Funktionen zur Bedrohungserkennung kann Ihr Netzwerk durch die Möglichkeit zur Integration mit anderen McAfee-Sicherheitsprodukten vor Malware und weiteren hochentwickelten, andauernden Bedrohungen (Advanced Persistent Threats, APTs) geschützt werden.

Inhalt

- *Das Malware-Bedrohungsszenario*
- *Die McAfee Advanced Threat Defense-Lösung*

Das Malware-Bedrohungsszenario

Unter den Begriff Malware fällt jede Software mit der Fähigkeit, bösartige Aktionen gegen einen Computer, eine Anwendung oder ein Netzwerk auszuführen. McAfee Advanced Threat Defense wurde zur Erkennung dateibasierter Malware entwickelt.

Früher erhielten Benutzer Malware in E-Mail-Anhängen. Mit dem Anstieg an Internetanwendungen müssen Benutzer nur noch auf einen Link klicken, um Dateien herunterzuladen. Heute gibt es viele andere Optionen, solche Dateien zu veröffentlichen: Blogs, Websites, Social-Networking-Websites,

Chat-Nachrichten, Webmail, Diskussionsforen und so weiter. Die große Herausforderung beim Angehen dieses Problems ist das Erkennen von Malware in der kürzestmöglichen Zeit und das Verhindern einer Ausbreitung auf andere Computer.

Eine Malware-Schutzstrategie umfasst vier Hauptaspekte:

- Erkennen von Datei-Downloads: Wenn ein Benutzer eine Datei von einer externen Ressource herunterlädt, muss Ihr Sicherheitsprodukt in der Lage sein, diesen Download zu erkennen.
- Analyse der Datei auf Malware: Sie müssen überprüfen können, ob die Datei bekannte Malware enthält.
- Blockieren zukünftiger Downloads der gleichen Datei: Wenn die Datei als bösartig erkannt wird, muss Ihr Malware-Schutz anschließend zukünftige Downloads der gleichen Datei oder Varianten davon verhindern.
- Identifizieren betroffener Hosts und Problembehebung: Ihr Sicherheitssystem muss den Host identifizieren können, der die Malware ausgeführt hat, und auch die Hosts ermitteln, auf die sie sich ausgebreitet hat. Anschließend muss es in der Lage sein, die betroffenen Hosts zu isolieren, bis sie gesäubert sind.

Die McAfee Advanced Threat Defense-Lösung

Eine Sicherheitslösung, die auf einer einzelnen Methode oder einem einzelnen Prozess basiert, reicht möglicherweise nicht zum verlässlichen Schutz vor Malware-Angriffen aus. Sie benötigen dazu eventuell eine mehrschichtige Lösung mit verschiedenen Techniken und Produkten. Bei einer solchen Lösung können Musterabgleich, globale Reputation, Programmemulation sowie statische und dynamische Analysen zum Einsatz kommen. Diese verschiedenen Schichten müssen nahtlos integriert und von einem Ort aus steuerbar sein, damit die einfache Konfiguration und Verwaltung gewährleistet sind. Durch Musterabgleich sind beispielsweise Zero-Day-Angriffe nicht erkennbar. Und während statische Analysen weniger Zeit in Anspruch nehmen als dynamische, kann Malware diese durch Codeverschleierung umgehen. Malware kann auch die Entdeckung durch dynamische Analysen verhindern, indem sie die Ausführung verzögert oder einen alternativen Ausführungspfad benutzt, wenn sie erkennt, dass sie in einer Sandkastenumgebung ausgeführt wird. Aus diesen Gründen erfordert ein zuverlässiger Malware-Schutz einen mehrschichtigen Ansatz.

Es gibt auch andere marktführende Malware-Schutzprodukte von McAfee für Web, Netzwerk und Endpunkte. McAfee hat allerdings erkannt, dass eine leistungsstarke Malware-Schutzlösung einen mehrschichtigen Ansatz erfordert. Das Ergebnis ist McAfee Advanced Threat Defense.

Die McAfee Advanced Threat Defense-Lösung besteht im Wesentlichen aus der McAfee Advanced Threat Defense Appliance und der vorinstallierten Software. Die McAfee Advanced Threat Defense Appliance ist in zwei Versionen verfügbar. Das Standardmodell ist ATD-3000. Das High-End-Modell ist ATD-6000.

McAfee Advanced Threat Defense integriert die eigenen Funktionen nahtlos in andere McAfee-Produkte und bietet Ihnen somit eine mehrschichtige Malware-Schutzstrategie:

- Der Ersterkennungsmechanismus besteht aus einer lokalen Blacklist, die bekannte Malware schnell erkennt.
- Zum Nachschlagen von Malware in der Cloud, die bereits von anderen Unternehmen weltweit erkannt wurde, ist eine Integration in McAfee® Global Threat Intelligence™ (McAfee GTI) möglich.
- Für Emulationen ist die McAfee Gateway Anti-Malware Engine eingebettet.

- Für die signaturbasierte Erkennung ist McAfee Anti-Malware Engine eingebettet.
- Dateien werden durch Ausführung in einer virtuellen Sandkastenumgebung dynamisch analysiert. McAfee Advanced Threat Defense bestimmt aufgrund des Verhaltens der Datei, ob die Datei bösartig ist.

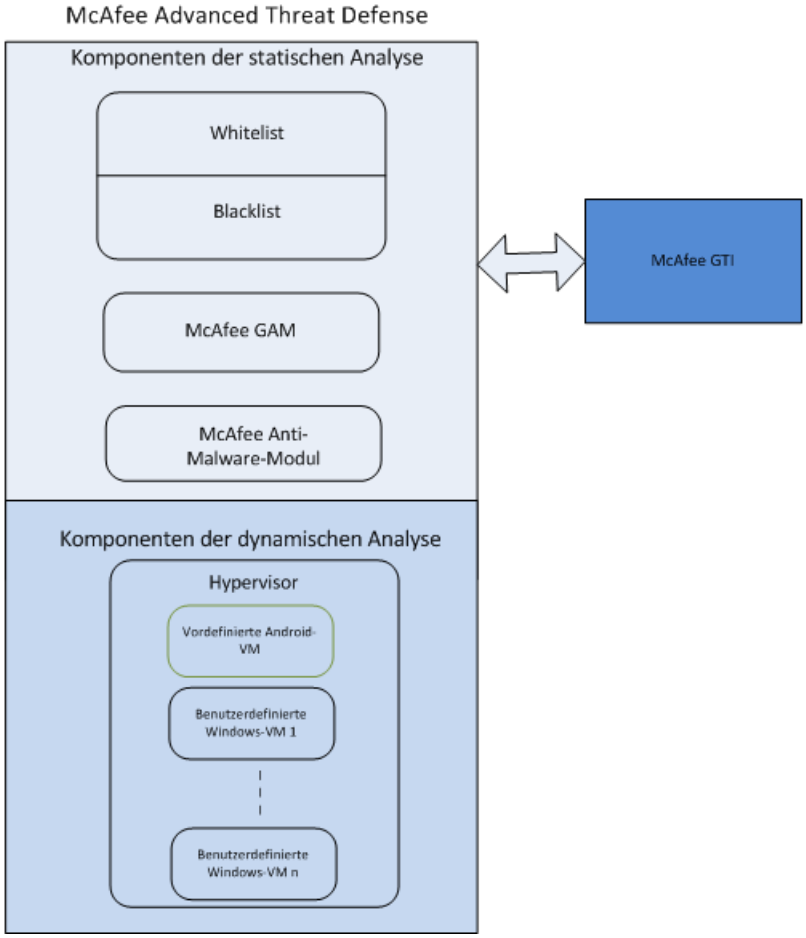


Abbildung 1-1 Komponenten für die Malware-Analyse

McAfee Advanced Threat Defense-Bereitstellungsoptionen

Sie können McAfee Advanced Threat Defense wie folgt bereitstellen:

- Standalone-Bereitstellung – Dies ist eine einfache Möglichkeit der Bereitstellung von McAfee Advanced Threat Defense. In diesem Fall erfolgt keine Integrierung in andere extern installierte McAfee-Produkte. Bei einer eigenständigen Appliance (Standalone) können Sie die verdächtigen Dateien manuell über die McAfee Advanced Threat Defense-Web-Anwendung senden. Alternativ können Sie die Proben über einen FTP-Client senden. Diese Bereitstellungsoption wird beispielsweise während der Test- und Auswertungsphase verwendet, um die Konfiguration zu präzisieren und verdächtige Dateien in einem isolierten Netzwerksegment zu analysieren. Forscher könnten die Standalone-Bereitstellung zudem für die detaillierte Malware-Analyse verwenden.

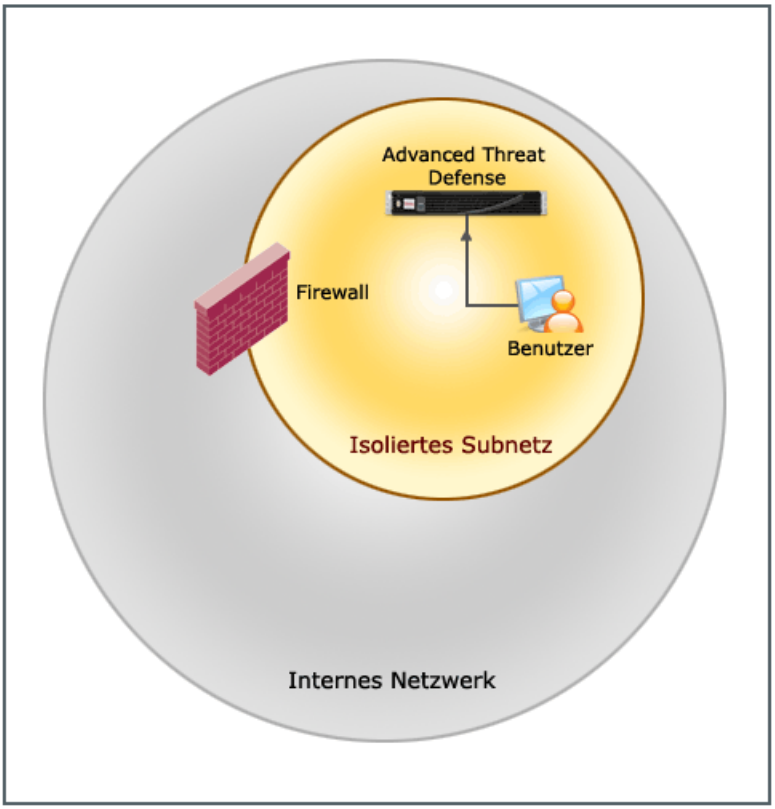


Abbildung 1-2 Standalone-Bereitstellungsszenario

- Integration in Network Security Platform – Diese Bereitstellung beinhaltet die Integration von McAfee Advanced Threat Defense in Network Security Platform-Sensor und -Manager.

  Abhängig von der Konfiguration der entsprechenden erweiterten Malware-Richtlinie erkennt ein Inline-Sensor einen Datei-Download und sendet eine Kopie der Datei zur Analyse an McAfee Advanced Threat Defense. Falls McAfee Advanced Threat Defense innerhalb weniger Sekunden Malware erkennt, kann der Sensor den Download blockieren. Der Manager zeigt die Ergebnisse der Analyse von McAfee Advanced Threat Defense an.

  Wenn McAfee Advanced Threat Defense mehr Zeit zur Analyse benötigt, lässt der Sensor den Datei-Download zu. Wenn McAfee Advanced Threat Defense Malware erkennt, nachdem die Datei heruntergeladen wurde, wird eine Information anNetwork Security Platform gesendet. Sie können den Sensor verwenden, um den Host zu isolieren, bis er gesäubert und das Problem behoben wurde. Sie können den Manager so konfigurieren, dass alle Sensoren für diese bösartige Datei aktualisiert werden. Dadurch blockieren Ihre Sensoren diese Datei möglicherweise wieder, wenn sie an einer anderen Stelle in Ihrem Netzwerk erneut heruntergeladen wird.

  Informationen zur Integration von Network Security Platform in McAfee Advanced Threat Defense finden Sie im *Network Security Platform-Integrationshandbuch.*

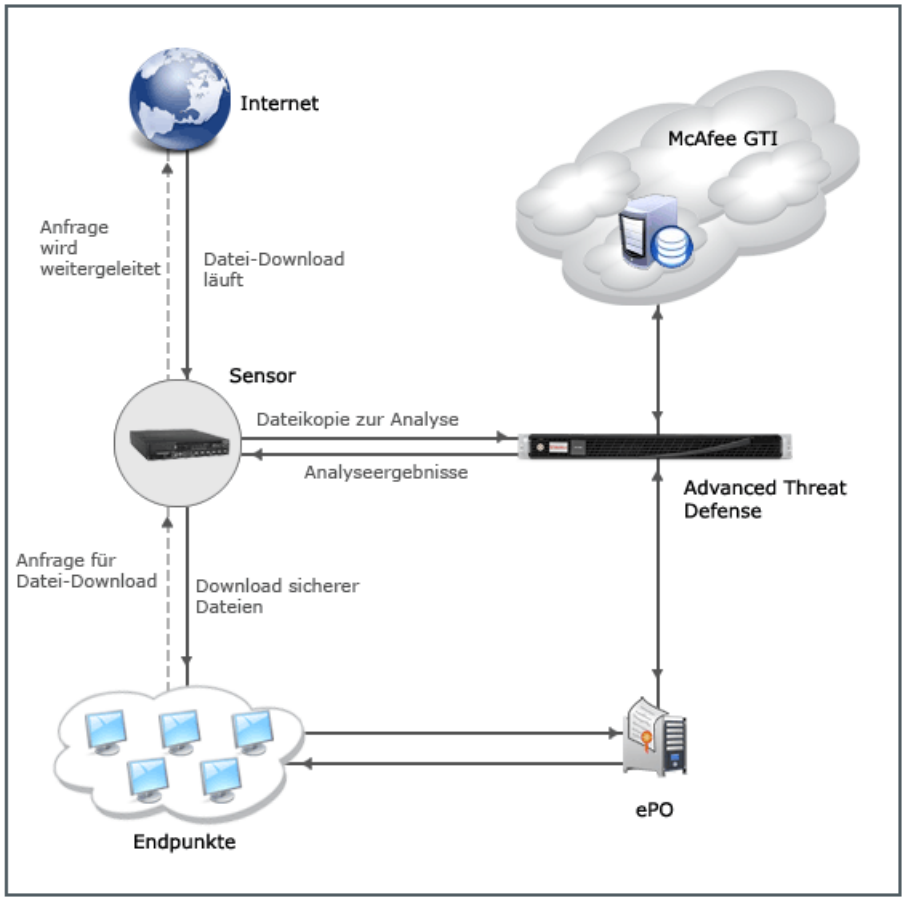


Abbildung 1-3 Integration in Network Security Platform und McAfee ePO

- Integration in McAfee® Web Gateway – Sie können McAfee Advanced Threat Defense als zusätzliches Modul für den Malware-Schutz konfigurieren. Wenn Ihr Netzwerkbenutzer eine Datei herunterlädt, scannt die native McAfee Gateway Anti-Malware Engine auf McAfee® Web Gateway die Datei und ermittelt einen Malware-Faktor. Abhängig von diesem Faktor und dem Dateityp sendet McAfee® Web Gateway eine Kopie der Datei zur genaueren Prüfung und dynamischen Analyse an McAfee Advanced Threat Defense. Eine Fortschrittsseite informiert Ihre Benutzer, dass die angeforderte Datei auf Malware überprüft wird. Abhängig von dem Malware-Schweregrad, der von McAfee Advanced Threat Defense ermittelt wurde, legt McAfee® Web Gateway fest, ob die Datei zugelassen oder blockiert wird. Bei einer Blockierung werden Ihren Benutzern die Gründe dafür angezeigt. Die Details zur erkannten Malware können Sie in der Protokolldatei einsehen.

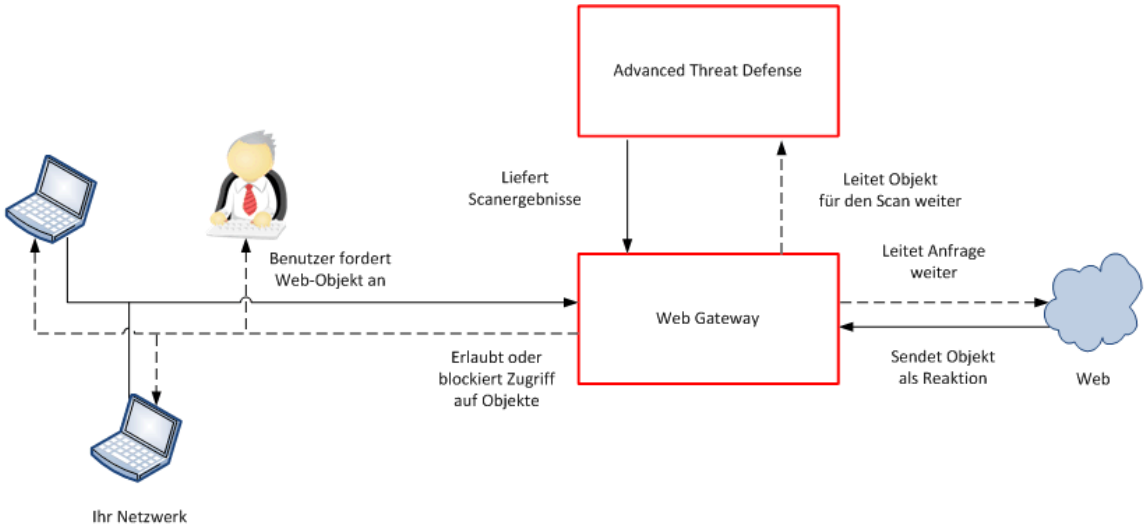


Abbildung 1-4 Integration in McAfee® Web Gateway

Durch diesen Ansatz wird sichergestellt, dass nur Dateien, die eine eingehende Analyse erfordern, an McAfee Advanced Threat Defense gesendet werden. Für den Benutzer bedeutet das ein Gleichgewicht zwischen Downloadgeschwindigkeit und Sicherheit. Informationen zur Integration von McAfee Advanced Threat Defense in McAfee® Web Gateway finden Sie im *McAfee® Web Gateway-Produkthandbuch*, Version 7.4.

- Integration in McAfee® ePolicy Orchestrator (McAfee ePO) – Ermöglicht McAfee Advanced Threat Defense, Informationen zum Zielhost abzurufen. Wenn das Betriebssystem auf dem Zielhost bekannt ist, kann für die dynamische Analyse eine ähnliche virtuelle Umgebung ausgewählt werden.

- Integration in McAfee® Next Generation Firewall (McAfee NGFW) – McAfee Next Generation Firewall integriert Sicherheitsfunktionen mit hoher Verfügbarkeit und Verwaltbarkeit. Sie integriert Application Control, Intrusion Prevention System (IPS) und Umgehungsprävention in eine einzige, preiswerte Lösung. Folgende Schritte sollten von McAfee Next Generation Firewall-Kunden

durchgeführt werden, um McAfee Next Generation Firewall in McAfee Advanced Threat Defense zu integrieren:

1. Erstellen Sie einen Advanced Threat Defense-Benutzer mit dem Namen "ngfw", nachdem Sie sich als Administrator bei Advanced Threat Defense angemeldet haben. Dieser Benutzer verfügt über dieselben Berechtigungen wie der Benutzer "nsp".
2. Starten Sie amas von der CLI aus neu.
3. Verwenden Sie im SCM den Benutzer "ngfw", um REST-API-Aufrufe auszuführen.



Es werden keine Änderungen am bestehenden SOFA-Protokoll zur Dateiübertragung vorgenommen. Da ein Benutzer mit dem Namen "ngfw" existiert, wird davon ausgegangen, dass alle Datenübertragungen über den SOFA-Kanal von McAfee NGFW-Appliances erfolgen.



Die Advanced Threat Defense kann McAfee Network Security Platform und McAfee Next Generation Firewall nicht in derselben Umgebung unterstützen.

Die Bereitstellungsoptionen behandeln die vier Hauptaspekte des Malware-Schutz-Prozesszyklus wie folgt:

- Erkennen eines Datei-Downloads: Sobald ein Benutzer auf eine Datei zugreift, erkennt der Network Security Platform-Inline-Sensor oder McAfee® Web Gateway dies und sendet eine Kopie der Datei an McAfee Advanced Threat Defense zur Analyse.
- Analyse der Datei auf Malware: Bevor der Benutzer die Datei vollständig heruntergeladen hat, kann McAfee Advanced Threat Defense eine bekannte Malware mithilfe von lokalen oder Cloudressourcen erkennen.
- Blockieren zukünftiger Downloads der gleichen Datei: Jedes Mal, wenn McAfee Advanced Threat Defense Malware mit mittlerem, hohem oder sehr hohem Schweregrad erkennt, wird die lokale Blacklist aktualisiert.
- Identifizieren betroffener Hosts und Problembehebung: Die Integration in Network Security Platform ermöglicht die Isolierung des Hosts, bis er gesäubert und das Problem behoben ist.

Vorteile von McAfee Advanced Threat Defense

McAfee Advanced Threat Defense bietet unter anderem folgende Vorteile:

- Es handelt sich um eine lokale Lösung mit Zugriff auf cloudbasierte GTI. Darüber hinaus kann diese auch in andere Sicherheitsprodukte von McAfee integriert werden.
- McAfee Advanced Threat Defense beeinträchtigt nicht den Datenverkehr in Ihrem Netzwerk. Die Lösung analysiert an sie gesendete Dateien bezüglich Malware. Das bedeutet, dass Sie die McAfee Advanced Threat Defense Appliance an einem beliebigen Ort in Ihrem Netzwerk installieren können, auf den alle integrierten McAfee-Produkte Zugriff haben. Es ist auch möglich, dass eine McAfee Advanced Threat Defense Appliance für alle integrierten Produkte benutzt wird (vorausgesetzt, dass die Anzahl der gesendeten Dateien innerhalb der Supportstufe liegt). Aufgrund dieser Struktur kann die Lösung als kosteneffizienter und skalierbarer Malware-Schutz eingesetzt werden.
- McAfee Advanced Threat Defense ist kein Inline-Gerät. Das Programm erhält von IPS-Sensoren Dateien zur Malware-Analyse. Dadurch kann McAfee Advanced Threat Defense so bereitgestellt werden, dass Sie die Vorteile einer Malware-Schutz-Inline-Lösung nutzen können, ohne die damit verbundenen Nachteile zu haben.
- Android ist derzeit eines der Hauptziele von Malware-Entwicklern. Dank dieser Integration sind die Android-basierten Handheld-Geräte in Ihrem Netzwerk ebenfalls geschützt. Dateien, die durch Android-Geräte (beispielsweise Smartphones und Tablets) heruntergeladen werden, können dynamisch analysiert werden.

- Dabei werden Dateien von mehreren Modulen gleichzeitig analysiert. Dadurch wird bekannte Malware beinahe in Echtzeit blockiert.
- Wenn McAfee Advanced Threat Defense eine Datei dynamisch analysiert, wählt das Programm den virtuellen Analysecomputer aus, auf dem dasselbe Betriebssystem und die gleichen sonstigen Anwendungen wie auf dem Zielhost installiert sind. Dies geschieht durch die Integration in McAfee ePO oder durch die Funktion zur passiven Geräteprofilerstellung in Network Security Platform. Dadurch können Sie die genauen Auswirkungen auf den Zielhost ermitteln und die erforderlichen Abhilfemaßnahmen ergreifen. Eine weitere Folge dieser Vorgehensweise ist, dass McAfee Advanced Threat Defense die Datei nur auf dem erforderlichen virtuellen Computer ausführt und Ressourcen für andere Dateien geschont werden.
- Stellen Sie sich folgende Situation vor: Ein Host lädt eine Zero-Day-Malware herunter, die jedoch von einem Sensor erkannt wird. Der Sensor leitet die heruntergeladene Datei an McAfee Advanced Threat Defense weiter. Die dynamische Analyse durch McAfee Advanced Threat Defense ergibt, dass die Datei bösartig ist. Je nach Ihren Einstellungen für die erweiterte Malware-Richtlinie kann der Manager diese Malware der Blacklist für alle Sensoren im Netzwerk Ihres Unternehmens hinzufügen. Die Datei befindet sich möglicherweise auch in der Blacklist von McAfee Advanced Threat Defense. Dadurch wird die Möglichkeit, dass dieselbe Datei noch einmal in Ihr Netzwerk gelangt, begrenzt.
- Eine Zero-Day-Malware kann sogar beim ersten Herunterladen eingedämmt werden, indem die betroffenen Hosts isoliert werden, bis sie gesäubert sind und das Problem behoben wurde.
- Durch Packen kann die Zusammensetzung des Codes verändert oder der Malware Reverse Engineering ermöglicht werden. Daher ist das richtige Entpacken sehr wichtig, um den tatsächlichen Malware-Code für die Analyse zu erhalten. McAfee Advanced Threat Defense ist in der Lage, den Code so zu entpacken, dass der Originalcode für die statische Analyse gesichert wird.

2

Einrichten der McAfee Advanced Threat Defense Appliance

In diesem Kapitel erhalten Sie Informationen zur McAfee Advanced Threat Defense Appliance und deren Einrichtung.

Inhalt

- *Über die McAfee Advanced Threat Defense-Appliance*
- *Funktionen einer McAfee Advanced Threat Defense-Appliance*
- *Vor dem Installieren der McAfee Advanced Threat Defense Appliance*
- *Hardware-Spezifikationen und Umgebungsanforderungen*
- *Einrichten der McAfee Advanced Threat Defense*

Über die McAfee Advanced Threat Defense-Appliance

Die McAfee Advanced Threat Defense-Appliance ist je nach Modell ein kompaktes 1-HE- oder 2-HE-Rackchassis mit einem Prozessor der Produktfamilie Intel® Xeon® E5-2600. Sie läuft mit einem vorinstallierten, stabilen Kernel von Linux 3.6.0 und wird mit der McAfee Advanced Threat Defense-Software geliefert.

Die McAfee Advanced Threat Defense-Appliance ist in den folgenden Modellen verfügbar:

- ATD-3000: Dieses Standardmodell ist ein 1-HE-Chassis.
- ATD-6000: Dieses High-End-Modell ist ein 2-HE-Chassis.

Funktionen einer McAfee Advanced Threat Defense-Appliance

Die McAfee Advanced Threat Defense-Appliances sind speziell angefertigte, skalierbare und flexible Hochleistungsserver für die Analyse verdächtiger Dateien auf Malware.

Dies sind die Hauptfunktionen der McAfee Advanced Threat Defense-Appliance:

- Hosten der McAfee Advanced Threat Defense-Software, die Dateien auf Malware analysiert
- Hosten der McAfee Advanced Threat Defense-Web-Anwendung
- Hosten der virtuellen Computer, die für die dynamische Analyse verdächtiger Dateien verwendet werden

Informationen zu den Leistungswerten von ATD-3000 und ATD-6000 erhalten Sie vom McAfee-Support.

Vor dem Installieren der McAfee Advanced Threat Defense Appliance

In diesem Abschnitt werden die Aufgaben beschrieben, die vor der Installation von McAfee Advanced Threat Defense ausgeführt werden müssen.

- Lesen Sie vor der Installation die mitgelieferte Dokumentation.
- Stellen Sie sicher, dass Sie einen geeigneten Speicherort für die Installation der McAfee Advanced Threat Defense Appliance gewählt haben.
- Überprüfen Sie, dass Sie alle notwendigen Ausrüstungsteile und Komponenten haben, die in diesem Dokument aufgeführt sind.
- Machen Sie sich mithilfe dieses Dokuments mit den NIC-Anschlüssen und Steckern der McAfee Advanced Threat Defense Appliance vertraut.
- Stellen Sie sicher, dass Sie folgende Informationen zur Hand haben, wenn Sie die McAfee Advanced Threat Defense Appliance konfigurieren:
  - IPv4-Adresse, die Sie der Appliance zuweisen möchten
  - Netzwerkmaske
  - Standard-Gateway-Adresse

Warnungen und Hinweise

Lesen und beachten Sie diese Sicherheitswarnungen, wenn Sie die McAfee Advanced Threat Defense-Appliance installieren. Ein Nichtbeachten dieser Sicherheitswarnungen kann zu ernsthaften Personenschäden führen.



Ein-/Aus-Schalter der McAfee Advanced Threat Defense-Appliance – Der Ein-/Aus-Schalter auf der Vorderseite der McAfee Advanced Threat Defense-Appliance schaltet nicht die Stromversorgung ab. Um die Stromversorgung für die McAfee Advanced Threat Defense-Appliance abzuschalten, müssen Sie beide Netzkabel von der Stromquelle oder den Steckdosen trennen.



Die Stromversorgung in Ihrem System kann eine Gefahr durch hohe Spannungen und Stromschlag darstellen und zu Personenschaden führen. Nur geschulte Techniker sind autorisiert, die Abdeckungen zu entfernen und Komponenten innerhalb des Systems freizulegen.



Gefahrensituationen – Geräte und Kabel: Elektrische Gefahrensituationen können bei Strom-, Telefon- und Kommunikationskabeln entstehen. Schalten Sie die McAfee Advanced Threat Defense-Appliance aus und trennen Sie alle Telekommunikationssysteme, Netzwerke, Modems und beide Netzkabel von der McAfee Advanced Threat Defense-Appliance, bevor sie geöffnet wird. Anderenfalls können Verletzungen bei Personen oder Geräteschäden entstehen.



Vermeiden Sie Verletzungen – Das Anheben der McAfee Advanced Threat Defense-Appliance und die Rack-Montage ist eine Aufgabe für zwei Personen.



Dieses Gerät sollte geerdet werden. Stellen Sie sicher, dass der Host während des Normalbetriebs geerdet ist.



Entfernen Sie nicht die Außenhülle der McAfee Advanced Threat Defense-Appliance. Ein solches Vorgehen führt zum Erlöschen Ihrer Garantie.



Nehmen Sie das System nur in Betrieb, wenn alle Karten, Blenden sowie die vordere und rückwärtige Abdeckung ordnungsgemäß angebracht sind. Blenden und Abdeckplatten verhindern den Kontakt mit gefährlichen Spannungen und Stromkreisen im Chassis, dämmen elektromagentische Interferenzen ein, die zu Störungen bei anderen Geräten führen können, und leiten einen kühlenden Luftstrom durch das Chassis.



Um elektrische Schläge zu vermeiden, verbinden Sie keine Schutzkleinspannungen (SELV) mit Stromkreisen, die Telefonnetzspannung (TNV) führen. LAN-Anschlüsse enthalten SELV-Stromkreise, und WAN-Anschlüsse TNV-Kreise. Einige LAN- und WAN-Anschlüsse verwenden RJ-45-Stecker. Seien Sie beim Anschließen der Kabel vorsichtig.

Nutzungsbeschränkungen

Folgende Beschränkungen gelten für die Nutzung und den Betrieb der McAfee Advanced Threat Defense-Appliance:

- Entfernen Sie nicht die Außenhülle der McAfee Advanced Threat Defense-Appliance. Ein solches Vorgehen führt zum Erlöschen Ihrer Garantie.
- Die McAfee Advanced Threat Defense-Appliance ist kein Allzweck-Server.
- McAfee untersagt die Nutzung der McAfee Advanced Threat Defense-Appliance für andere Zwecke als den Betrieb der McAfee Advanced Threat Defense-Lösung.
- McAfee untersagt die Änderung oder Installation von Hardware oder Software in bzw. auf der McAfee Advanced Threat Defense-Appliance, sofern dies nicht im Rahmen des normalen Betriebs von McAfee Advanced Threat Defense passiert.

Auspacken der Lieferung

1 Öffnen Sie die Kiste.

2 Entnehmen Sie die erste Zubehörschachtel.

3 Überprüfen Sie, dass Sie alle unter Überprüfen der Lieferung auf Seite 22 aufgeführten Teile erhalten haben.

4 Entnehmen Sie die McAfee Advanced Threat Defense-Appliance.

5 Platzieren Sie die McAfee Advanced Threat Defense-Appliance so nahe wie möglich zum Installationsort.

6 Platzieren Sie die Schachtel so, dass die Schrift darauf richtig ausgerichtet ist.

7 Öffnen Sie die Klappen der Schachtel.

8 Entnehmen Sie die Zubehörschachtel aus der Schachtel, in der sich die McAfee Advanced Threat Defense-Appliance befindet.

9 Entfernen Sie den Gleitschienensatz.

10 Entfernen Sie das Verpackungsmaterial, das die McAfee Advanced Threat Defense-Appliance umgibt.

11 Nehmen Sie die McAfee Advanced Threat Defense-Appliance aus der antistatischen Tüte.

12 Heben Sie Schachtel und die Verpackungsmaterialien auf, falls Sie sie später für einen Umzug oder Versand der McAfee Advanced Threat Defense-Appliance benötigen.

Überprüfen der Lieferung

Die folgenden Zubehörteile sind in der Lieferung der McAfee Advanced Threat Defense Appliance enthalten:

- McAfee Advanced Threat Defense Appliance
- Im *Inhaltsblatt* aufgeführtes Zubehör
- Werkzeuglos zu montierender Laufschienensatz
- Frontblende mit Schlüssel

Vorder- und Rückseite der McAfee Advanced Threat Defense Appliance



Abbildung 2-1 Vorderansicht der ATD-3000 mit Blende



Abbildung 2-2 Seitenansicht der ATD-3000 ohne Blende

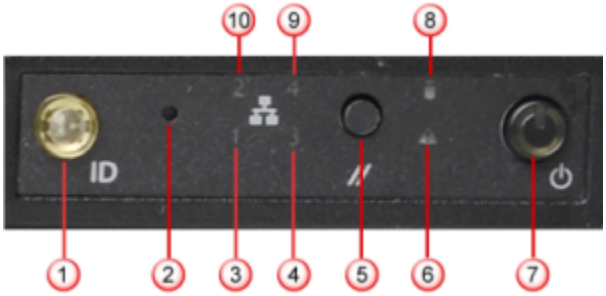


Abbildung 2-3 Vorderseite der ATD-3000 und ATD-6000

Beschriftung	Beschreibung
1	System-ID-Taste mit integrierter LED-Anzeige
2	NMI-Taste (zurückgesetzt, Werkzeug erforderlich)
3	LED-Anzeige für NIC 1-Aktivität
4	• ATD-3000: LED-Anzeige für NIC 3-Aktivität • ATD-6000: Nicht verwendet
5	Taste für System-Kaltstart
6	Systemstatus-LED
7	Ein-/Ausschalter mit integrierter LED-Anzeige
8	LED-Anzeige für Festplattenaktivität
9	• ATD-3000: LED-Anzeige für NIC 4-Aktivität • ATD-6000: Nicht verwendet
10	LED-Anzeige für NIC 2-Aktivität

Im Lieferumfang der McAfee Advanced Threat Defense Appliance ist eine verschließbare Blende enthalten, mit der Sie die Vorderseite des Geräts abdecken können.

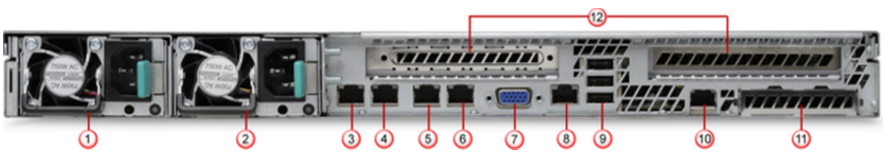


Abbildung 2-4 Rückseite der ATD-3000-Appliance

Beschriftung	Beschreibung
1	Stromversorgungsmodul 1
2	Stromversorgungsmodul 2
3	Verwaltungsport (NIC 1). Hierbei handelt es sich um die ETH-0-Schnittstelle. Die Befehle `set appliance` und `set mgmtport` gelten für diese Schnittstelle. Beispiel: Wenn Sie den Befehl `set appliance ip` verwenden, wird die entsprechende IP-Adresse dieser Schnittstelle zugewiesen.
4	NIC 2. Hierbei handelt es sich um die ETH-1-Schnittstelle. Diese Schnittstelle ist standardmäßig deaktiviert. • Um diese Schnittstelle zu aktivieren bzw. zu deaktivieren, verwenden Sie den Befehl `set intfport`. Beispiel: `set intfport 1 enable` • Um dieser Schnittstelle die IP-Daten zuzuweisen, verwenden Sie `set intfport <eth 1, 2, or 3> ip <IPv4 address> <subnet mask>`. Beispiel: `set intfport 1 ip 10.10.10.10 255.255.255.0` • Sie können diesem Port nicht das Standard-Gateway zuweisen. Sie können jedoch für diese Schnittstelle ein Routing konfigurieren, damit der Datenverkehr zum gewünschten Gateway geleitet wird. Um ein Routing zu konfigurieren, verwenden Sie `route add network <IPv4 subnet> netmask <netmask> gateway <IPv4 address> intfport 1`. Beispiel: `route add network 10.10.10.0 netmask 255.255.255.0 gateway 10.10.10.1 intfport 1`. Mit diesem Befehl wird der gesamte Datenverkehr des 10.10.10.0-Befehls über NIC 2 (ETH-1) an 10.10.10.1 geleitet.
5	NIC 3. Hierbei handelt es sich um die ETH-2-Schnittstelle. Siehe Beschreibung zu NIC 2.
6	NIC 4. Hierbei handelt es sich um die ETH-3-Schnittstelle. Siehe Beschreibung zu NIC 2.
7	Videoanschluss
8	RJ-45-Anschluss (seriell)
9	USB-Anschlüsse
10	RMM4 NIC-Anschluss
11	Anschlüsse/Buchsen für E/A-Modul (nicht verwendet)
12	Add-in-Adapter-Slots von Riser Card 1 und 2

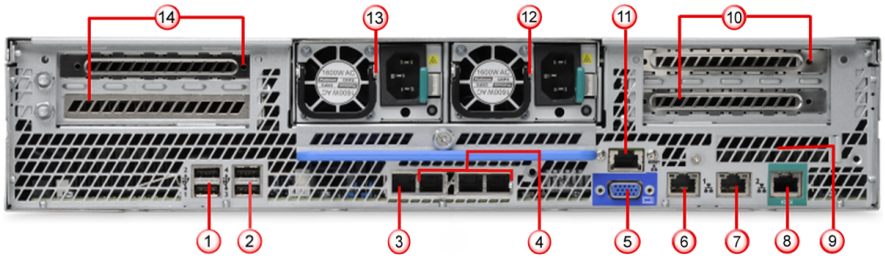


Abbildung 2-5 Rückseite der ATD-6000-Appliance

Beschriftung	Beschreibung
1	USB-Anschlüsse
2	USB-Anschlüsse

Beschriftung	Beschreibung
3	Verwaltungsport: Hierbei handelt es sich um die ETH-0-Schnittstelle. Die Befehle `set appliance` und `set mgmtport` gelten für diese Schnittstelle. Beispiel: Wenn Sie den Befehl `set appliance ip` verwenden, wird die entsprechende IP-Adresse dieser Schnittstelle zugewiesen.
4	Zusätzliche Anschlüsse/Buchsen für E/A-Modul. Hierbei handelt es sich jeweils um die ETH-1-, ETH-2- und ETH-3-Schnittstellen. Diese Schnittstellen sind standardmäßig deaktiviert. • Um eine Schnittstelle zu aktivieren bzw. zu deaktivieren, verwenden Sie den Befehl `set intfport`. Zum Beispiel aktivieren Sie ETH-1 mit `set intfport 1 enable`. • Um einer Schnittstelle die IP-Daten zuzuweisen, verwenden Sie `set intfport <eth 1, 2, or 3> ip <IPv4 address> <subnet mask>`. Beispiel: `set intfport 1 ip 10.10.10.10 255.255.255.0` • Sie können diesem Port nicht das Standard-Gateway zuweisen. Sie können jedoch für diese Schnittstelle ein Routing konfigurieren, damit der Datenverkehr zum gewünschten Gateway geleitet wird. Um ein Routing zu konfigurieren, verwenden Sie `route add network <IPv4 subnet> netmask <netmask> gateway <IPv4 address> intfport 1`. Beispiel: `route add network 10.10.10.0 netmask 255.255.255.0 gateway 10.10.10.1 intfport 1`. Mit diesem Befehl wird der gesamte Datenverkehr des 10.10.10.0-Befehls über NIC 2 (ETH-1) an 10.10.10.1 geleitet.
5	Videoanschluss
6	NIC 1 (derzeit nicht verwendet)
7	NIC 2 (derzeit nicht verwendet)
8	RJ-45-Anschluss (seriell)
9	Anschlüsse/Buchsen für E/A-Modul (nicht verwendet)
10	Add-In-Adapter-Slots von Riser Card
11	RMM4 NIC-Anschluss
12	Stromversorgungsmodul 2
13	Stromversorgungsmodul 1
14	Add-In-Adapter-Slots von Riser Card

Hardware-Spezifikationen und Umgebungsanforderungen

Eigenschaften	ATD-3000	ATD-6000
Abmessungen	• 438 (B) x 43,2 (H) x 734,66 (L) mm • 43,82 (B) x 4,32 (H) x 73,66 (L) cm	• 438 (B) x 87,3 (H) x 712 (L) mm • 43,78 (B) × 8,71 (H) × 71,12 (L) cm
Formfaktor	1HE-Rack-Montage; für 19-Zoll-Gehäuse	2HE-Rack-Montage; für 19-Zoll-Gehäuse
Gewicht	15 kg	22,7 kg
Speicher	• Festplattenspeicher HDD: 2 x 4 TB • SSD: 2 x 400 GB	• Festplattenspeicher HDD: 4 x 4 TB • SSD: 2 x 800 GB
Maximaler Energieverbrauch	2 x 750 W	2 x 1.600 W

Eigenschaften	ATD-3000	ATD-6000
Redundante Stromversorgung	Wechselstrom (redundant), im laufenden Betrieb austauschbar	Wechselstrom (redundant), im laufenden Betrieb austauschbar
Wechselspannung	100–240 V bei 50–60 Hz. 5,8 A	100–240 V. 50–60 Hz. 8,5 A
Betriebstemperatur	+10 °C bis +35 °C, wobei die Änderungsgeschwindigkeit maximal 10 °C pro Stunde beträgt	+10 °C bis +35 °C, wobei die Änderungsgeschwindigkeit maximal 10 °C pro Stunde beträgt
Lagerungstemperatur	-40 °C bis +70 °C	-40 °C bis +70 °C
Relative Feuchtigkeit (nicht kondensierend)	• In Betrieb: 10 bis 90 Prozent • Außer Betrieb: 90 Prozent bei 35 °C	• In Betrieb: 10 bis 90 Prozent • Außer Betrieb: 50 bis 90 Prozent bei einer maximalen Feuchttemperatur von 28 °C (bei Temperaturen zwischen 25 °C und 35 °C)
Höhe	Betrieb wird in einer Höhe von bis zu 3.050 Metern unterstützt	Betrieb wird in einer Höhe von bis zu 3.050 Metern unterstützt
Sicherheitszertifizierung	UL 1950, CSA-C22.2 Nr. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB-Lizenz und -Report zur Abdeckung aller nationalen Abweichungen	UL 1950, CSA-C22.2 Nr. 950, EN-60950, IEC 950, EN 60825, 21CFR1040 CB-Lizenz und -Report zur Abdeckung aller nationalen Abweichungen
EMI-Zertifizierung	FCC Teil 15, Klasse A (CFR 47) (USA) ICES-003 Klasse A (Kanada), EN55022 Klasse A (Europa), CISPR22 Klasse A (International)	FCC Teil 15, Klasse A (CFR 47) (USA) ICES-003 Klasse A (Kanada), EN55022 Klasse A (Europa), CISPR22 Klasse A (International)
Akustik	Schallleistung: 7,0 BA bei einer typischen Umgebungstemperatur in Büros (23 +/- 2 °C)	Schallleistung: 7,0 BA bei einer typischen Umgebungstemperatur in Büros (23 +/- 2 °C)
Erschütterung, im Betrieb	Halbsinus, 2 g Höchstwert, 11 Millisekunden	Halbsinus, 2 g Höchstwert, 11 Millisekunden
Erschütterung, unverpackt	Trapezoid, 25 g, Geschwindigkeitsänderung 3,45 m/ Sekunde (≧18,1 kg bis < 36,3 kg)	Trapezoid, 25 g, Geschwindigkeitsänderung basiert auf Gewicht mit Verpackung
Erschütterung, verpackt	Nicht palettierter freier Fall aus einer Höhe von 0,7 Metern (≧18,1 kg bis < 36,3 kg)	• Produktgewicht: ≥ 18,1 bis < 36,3 • Nicht palettierter freier Fall aus einer Höhe von 0,5 Metern • Palettiert (Einzelprodukt) Freifallhöhe = keine Angabe
Vibration	Unverpackt: 5 Hz bis 500 Hz, 2,20 g RMS regellos	Unverpackt: 5 Hz bis 500 Hz, 2,20 g RMS regellos Verpackt: 5 Hz bis 500 Hz, 1,09 g RMS regellos
ESD	+/-12 kV außer E/A-Port +/- 8 kV laut Informationen aus Intel®-Umwelttests	Luftentladung: 12,0 kV Kontaktentladung: 8,0 kV
Kühlbedarf des Systems in BTU/Std.	• 460 Watt Max bis 1.570 BTU/Std. • 750 Watt Max bis 2.560 BTU/Std.	• 460 Watt Max bis 1.570 BTU/Std. • 750 Watt Max bis 2.560 BTU/Std.
Arbeitsspeicher	192 GB	256 GB

Portnummern

Tabelle 2-1 Portnummern

Client	Server	Standardport	Konfigurierbar	Beschreibung
Beliebig (Desktop)	McAfee Advanced Threat Defense	TCP 443 (HTTPS)	Nein	Zugriff auf die McAfee Advanced Threat Defense-Web-Anwendung
Beliebig (FTP-Client)	McAfee Advanced Threat Defense	TCP 22 (SFTP)	Nein	Zugriff auf den FTP-Server auf McAfee Advanced Threat Defense
Sensor	McAfee Advanced Threat Defense	TCP 8505	Nein	Kommunikationskanal zwischen einem Sensor und McAfee Advanced Threat Defense
Manager	McAfee Advanced Threat Defense	TCP 443 (HTTPS)	Nein	Kommunikation zwischen dem Manager und McAfee Advanced Threat Defense über die REST-APIs
McAfee Advanced Threat Defense	McAfee ePO	TCP 8443	Ja	Hostdatenabfragen.
McAfee Advanced Threat Defense	`tunnel.message.trustedsource.org`	TCP 443 (HTTPS)	Nein	Datei-Reputations-Abfragen.
McAfee Advanced Threat Defense	`List.smartfilter.com`	TCP 80 (HTTP)	Nein	URL-Aktualisierungen.
Beliebig (SSH-Client)	McAfee Advanced Threat Defense	TCP 2222 (SSH)	Nein	CLI-Zugriff
McAfee Advanced Threat Defense	`wpm.webwasher.com`	TCP 443 (HTTPS)	Nein	Aktualisierungen für McAfee Gateway Anti-Malware Engine und McAfee Anti-Malware Engine.

Einrichten der McAfee Advanced Threat Defense

In diesem Kapitel wird beschrieben, wie die McAfee Advanced Threat Defense Appliance eingerichtet wird, damit Sie sie konfigurieren können.

Inhalt

- *Montieren und Entfernen von Rackgriffen*
- *Installieren oder Entfernen der Appliance aus dem Rack*
- *Einschalten der McAfee Advanced Threat Defense Appliance*
- *Umgang mit der Frontblende*
- *Verbinden des Netzwerkkabels*
- *Konfigurieren der Netzwerkinformationen für die McAfee Advanced Threat Defense Appliance*

Montieren und Entfernen von Rackgriffen

- Um einen Rackgriff zu montieren, richten Sie ihn an den beiden Löchern auf der Seite der McAfee Advanced Threat Defense-Appliance aus und befestigen Sie ihn gemäß Abbildung mithilfe von zwei Schrauben.

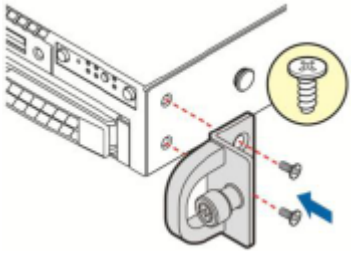


Abbildung 2-6 Installieren des Rackgriffs

- Zum Entfernen eines Rackgriffs entfernen Sie die beiden Schrauben, mit denen der Griff befestigt ist, und entfernen Sie den Rack-Griff wie gezeigt vom Serversystem.

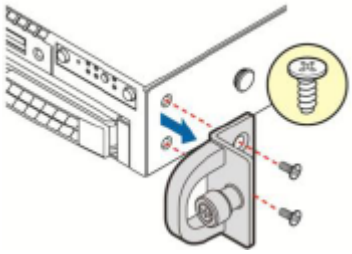


Abbildung 2-7 Entfernen des Rackgriffs

Installieren oder Entfernen der Appliance aus dem Rack

Installieren Sie die Appliance mithilfe des mit McAfee Advanced Threat Defense gelieferten Rackmontage-Sets in einem 19-Zoll-Montagerahmen. Das Montage-Set kann für die meisten Racks nach Industriestandard verwendet werden. Verwenden Sie die Kabelhalter zur Sicherung der Kabel der McAfee Advanced Threat Defense-Appliance im Rahmen.

Vorgehensweise

1 Platzieren Sie eine der Montageschienen so vorne im Rack, dass sich die Klemme auf der Höhe der entsprechenden Löcher im Rack befindet.

Beachten Sie die Sicherheitshinweise. Während Sie planen, wo im Rack Sie die McAfee Advanced Threat Defense-Appliance installieren möchten, denken Sie daran, dass Sie das Rack immer von unten nach oben beladen sollten. Wenn Sie mehrere McAfee Advanced Threat Defense-Appliances installieren, sollten Sie mit der untersten freien Stelle beginnen.

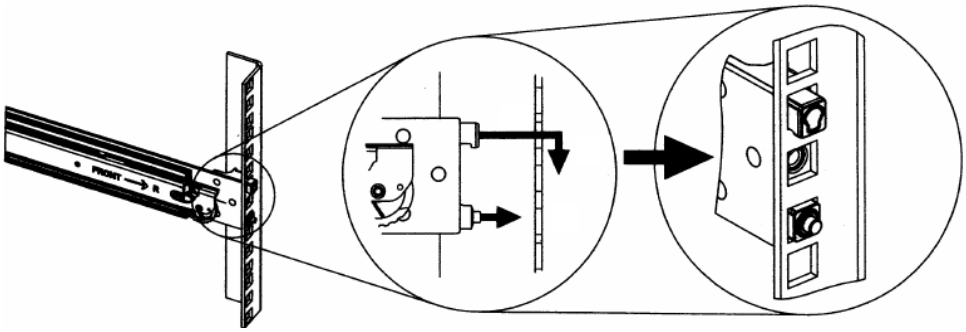


Abbildung 2-8 Installation der Gleitschiene

2 Ziehen Sie die Klemme an der Rückseite des Racks (und damit die Montageschiene) aus, und richten Sie sie an den entsprechenden Rack-Löchern aus.

Vergewissern Sie sich, das die Höhe der Montageschiene auf beiden Seiten des Racks gleich ist.

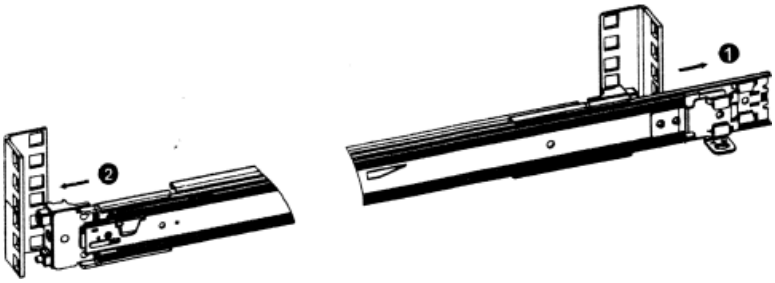


Abbildung 2-9 Installation der Schiene im Rack

3 Klemmen Sie die Schiene sicher am Rack fest.

4 Wiederholen Sie diese Schritte zum Befestigen der zweiten Montageschiene im Rack.

5 Ziehen Sie beide Schienen soweit wie möglich heraus.



Abbildung 2-10 Maximale Ausziehdistanz

6 Heben Sie die McAfee Advanced Threat Defense-Appliance mit der Hilfe einer zweiten Person an und installieren Sie das Chassis auf beiden Seiten gleichzeitig auf den Schienen.

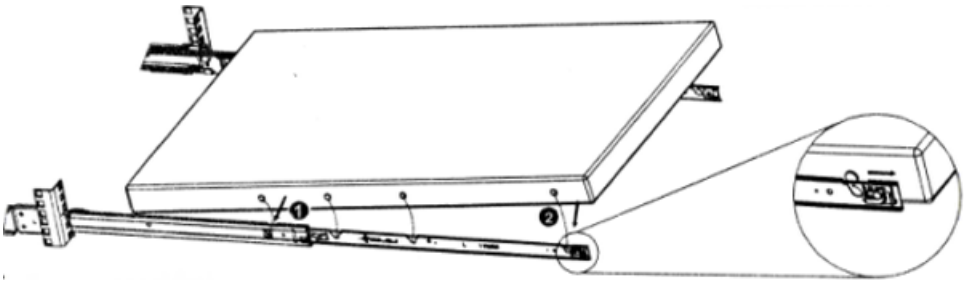


Abbildung 2-11 Installieren der Appliance auf den Schienen

Senken Sie zuerst die hintere Spule ab, gefolgt von der mittleren und dann der vorderen.

Das Anheben der McAfee Advanced Threat Defense-Appliance und das Befestigen im Rack erfordert zwei Personen.

7 Setzen Sie nötigenfalls die verschließbare Blende zum Schutz der Vorderseite auf.

8 Heben Sie die Entriegelungslasche an, und schieben Sie die Appliance in das Gestell.

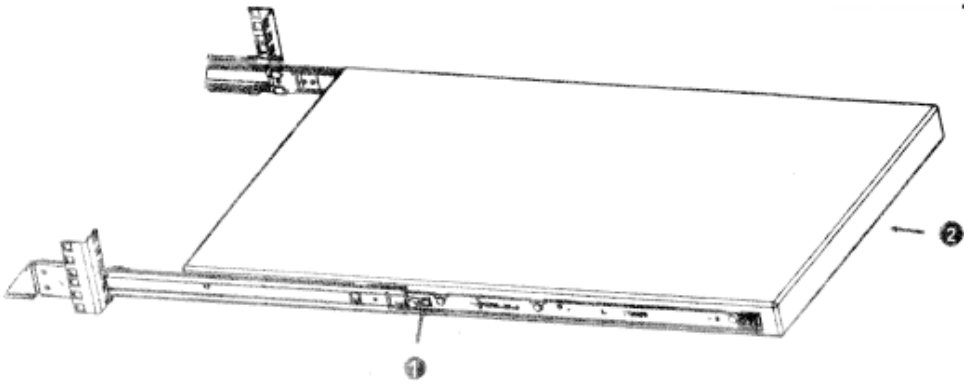


Abbildung 2-12 Entriegelungslasche anheben und Appliance in das Rack schieben

9 Zum Entfernen der McAfee Advanced Threat Defense-Appliance aus dem Rack heben Sie die Entriegelungslasche neben der vorderen Spule am Chassis an und heben Sie das Gerät aus den Schienen.

Dieser Vorgang muss auf beiden Seiten gleichzeitig erfolgen und erfordert zwei Personen.

Einschalten der McAfee Advanced Threat Defense Appliance

Die McAfee Advanced Threat Defense Appliance verfügt über vorinstallierte redundante Netzteile.

Die McAfee Advanced Threat Defense Appliance wird mit zwei Netzkabeln geliefert, die den Anforderungen Ihres Landes oder Ihrer Region entsprechen.

Vorgehensweise

1 Schließen Sie das eine Ende des Netzkabels an das erste Netzteilmodul auf der Rückseite und das andere Ende an eine geeignete Stromquelle an.

2 Schließen Sie das eine Ende des Netzkabels an das zweite Netzteilmodul auf der Rückseite und das andere Ende an eine geeignete Stromquelle an. Die McAfee Advanced Threat Defense wird eingeschaltet, ohne dass der Ein-/Ausschalter auf der Vorderseite betätigt werden muss.

Der Ein-/Ausschalter auf der Vorderseite schaltet nicht die Stromversorgung ein oder aus. Um die Stromversorgung für die McAfee Advanced Threat Defense Appliance abzuschalten, müssen Sie beide Netzkabel von der Stromversorgung oder den Steckdosen trennen.

Umgang mit der Frontblende

Sie können bei Bedarf die Frontblende entfernen und später wieder anbringen. Vor dem Anbringen müssen Sie jedoch die Rackgriffe montieren.

Vorgehensweise

1 Führen Sie folgende Schritte aus, um die Frontblende zu entfernen:

   a Lösen Sie gegebenenfalls die Verriegelung.

   b Entfernen Sie das linke Ende der Frontblende vom Rackgriff.

   c Drehen Sie die Frontblende gegen den Uhrzeigersinn, um die Klemmen rechts vom Rackgriff freizugeben.

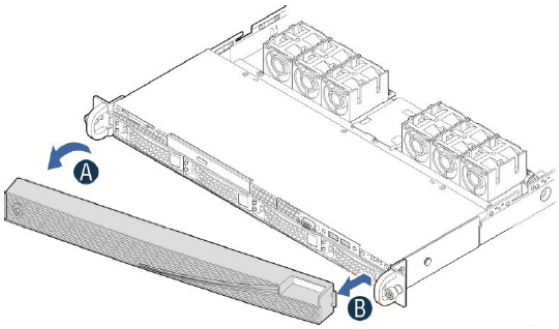


Abbildung 2-13 Entfernen der Frontblende

2 Führen Sie folgende Schritte aus, um die Frontblende anzubringen:

   a Lassen Sie das rechte Ende der Frontblende im Rackgriff einrasten.

   b Drehen Sie die Frontblende im Uhrzeigersinn, bis das linke Ende einrastet.

   c Verriegeln Sie die Blende bei Bedarf.

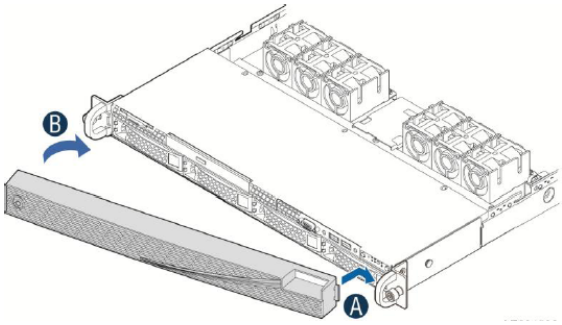


Abbildung 2-14 Anbringen der Frontblende

Verbinden des Netzwerkkabels

Vorgehensweise

1 Schließen Sie ein Ethernet-Kabel der Kategorie 5e oder 6 an den Verwaltungsport auf der Rückseite an.

2 Schließen Sie das andere Ende des Kabels an das entsprechende Netzwerkgerät an.

Konfigurieren der Netzwerkinformationen für die McAfee Advanced Threat Defense Appliance

Nach Abschluss der erstmaligen Installation und Konfiguration können Sie die McAfee Advanced Threat Defense Appliance über einen Remotecomputer oder Terminalserver verwalten. Dazu müssen Sie die McAfee Advanced Threat Defense Appliance mit den erforderlichen Netzwerkinformationen konfigurieren.

Vorgehensweise

1 Schließen Sie ein Konsolenkabel (RJ-45 auf DB-9, seriell) an den Konsolenanschluss (RJ-45, seriell) auf der Rückseite der McAfee Advanced Threat Defense Appliance an.

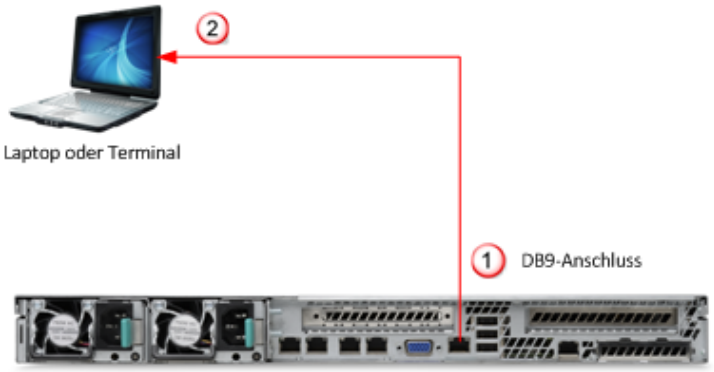


Abbildung 2-15 Verbinden des Konsolenanschlusses

2 Schließen Sie das andere Ende des Kabels direkt an den COM-Anschluss des PCs oder Terminal-Servers an, über den Sie die McAfee Advanced Threat Defense Appliance konfigurieren möchten.

3 Führen Sie HyperTerminal auf einem Microsoft Windows-Computer mit den folgenden Einstellungen aus:

Name	Einstellung
Baud-Rate	115200
Bitanzahl	8
Parität	Keine
Stopp-Bits	1
Ablaufsteuerung	Keine

4 Melden Sie sich auf Aufforderung bei der McAfee Advanced Threat Defense Appliance mit dem Standardbenutzernamen `cliadmin` und dem Kennwort `atdadmin` an.

Für Anweisungen zur Verwendung der integrierten Befehlssyntax-Hilfe geben Sie `help` oder `?` ein. Geben Sie `list` ein, um eine Liste aller Befehle zu erhalten.

5 Geben Sie in der Befehlszeile `set appliance name <Name>` ein, um den Namen der McAfee Advanced Threat Defense Appliance festzulegen.

Geben Sie die Werte zwischen den Zeichen <> ein, ohne <> einzugeben.

Beispiel: `set appliance name matd_appliance_1`

Der Name der McAfee Advanced Threat Defense Appliance kann eine Zeichenfolge von bis zu 25 alphanumerischen Zeichen sein. Die Zeichenfolge muss mit einem Buchstaben beginnen und darf Bindestriche, Unterstriche und Punkte enthalten, aber keine Leerzeichen.

6 Zum Festlegen der Verwaltungsport-IP-Adresse und Subnetzmaske der McAfee Advanced Threat Defense Appliance geben Sie `set appliance ip <A.B.C.D> <E.F.G.H>` ein.

Geben Sie eine 32-Bit-Adresse an, die als vier 8-Bit-Zahlen (durch Punkte getrennt) geschrieben ist. Beispiel: <A.B.C.D>, wobei A, B, C und D eine 8-Bit-Zahl zwischen 0 und 255 darstellen. <E.F.G.H> steht für die Subnetzmaske.

Beispiel: `set appliance ip 192.34.2.8 255.255.255.0`



Nach dem erstmaligen Festlegen oder einer Änderung der IP-Adresse muss die McAfee Advanced Threat Defense Appliance neu gestartet werden.

7 Geben Sie die Adresse des Standard-Gateways ein.

`set appliance gateway <A.B.C.D>`

Verwenden Sie die gleiche Konvention wie für den Befehl `set appliance ip`.

Beispiel: `set appliance gateway 192.34.2.1`

8 Legen Sie die Anschlussgeschwindigkeit und Duplexeinstellungen für den Verwaltungsport mithilfe eines der folgenden Befehle fest:

- `set mgmtport auto` – Stellt den Auto-Modus für Geschwindigkeit und Duplex des Verwaltungsports ein.
- `set mgmtport speed (10|100) duplex (full|half)` – Stellt die Geschwindigkeit auf 10 oder 100 Mbit/s bei Voll- oder Halb-Duplex ein.

9 Geben Sie zum Bestätigen der Konfiguration `show` ein.

Dies zeigt die derzeitigen Konfigurationsdetails an.

10 Senden Sie Ping-Befehle an andere Netzwerk-Hosts, um die Netzwerkverbindung zu überprüfen. Geben Sie auf die Aufforderung hin `ping <IP address>` ein.

Bei erfolgreichem Vorgang wird die Meldung `host <ip address> is alive` (Host <IP-Adresse> ist aktiv) angezeigt. Ist der Host nicht erreichbar, wird die Meldung `failed to talk to <ip address>` (Verbindung mit <IP-Adresse> fehlgeschlagen) angezeigt.

11 Ändern Sie das Kennwort für die McAfee Advanced Threat Defense Appliance mit dem Befehl `passwd`.

Das Kennwort muss zwischen 8 und 25 Zeichen umfassen und darf jedes alphanumerische Zeichen bzw. Symbol enthalten. Die Groß- und Kleinschreibung muss beachtet werden.



Es wird von McAfee dringend empfohlen, dass Sie ein Kennwort mit einer Zeichenkombination wählen, an die Sie sich einfach erinnern können, die jedoch für andere schwer zu erraten ist.

3

Zugreifen auf die McAfee Advanced Threat Defense-Web-Anwendung

Die McAfee Advanced Threat Defense-Web-Anwendung wird auf der McAfee Advanced Threat Defense-Appliance gehostet. Wenn Sie ein McAfee Advanced Threat Defense-Benutzer mit Web-Zugriff sind, können Sie von einem Remotecomputer mit einem unterstützten Browser auf die McAfee Advanced Threat Defense-Web-Anwendung zugreifen.

Die McAfee Advanced Threat Defense-Web-Anwendung bietet folgende Möglichkeiten:

- Überwachen von Zustand und Leistung derMcAfee Advanced Threat Defense-Appliance
- Verwalten der McAfee Advanced Threat Defense-Benutzer und ihrer Berechtigungen
- Konfigurieren von McAfee Advanced Threat Defense für die Malware-Analyse
- Manuelles Hochladen von Dateien zur Analyse
- Verfolgen des Analysefortschritts und anschließendes Anzeigen der Ergebnisse

Inhalt

- *McAfee Advanced Threat Defense-Client-Anforderungen*
- *Zugreifen auf die McAfee Advanced Threat Defense-Web-Anwendung*

McAfee Advanced Threat Defense-Client-Anforderungen

Für Client-Systeme, die auf die McAfee Advanced Threat Defense-Web-Anwendung zugreifen, gelten folgende Systemanforderungen:

- Client-Betriebssystem – Microsoft Windows XP, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows 7 und Microsoft Windows 8.0
- Browser – Internet Explorer 9 oder höher, Firefox und Chrome

Zugreifen auf die McAfee Advanced Threat Defense-Web-Anwendung

Vorgehensweise

1. Öffnen Sie auf einem Client-Computer über einen der unterstützten Browser eine Sitzung.
2. Nutzen Sie für den Zugriff auf die McAfee Advanced Threat Defense-Web-Anwendung folgende Daten:
   - URL – https://<McAfee Advanced Threat Defense Appliance-Hostname oder -IP-Adresse>
   - Standardbenutzername – `admin`
   - Kennwort – `admin`
3. Klicken Sie auf **Anmelden**.

4

Verwalten von Advanced Threat Defense

Zum Verwalten von Konfigurationen wie Benutzerkonten und zum Überwachen des Systemzustands von McAfee Advanced Threat Defense Appliance wird die McAfee Advanced Threat Defense-Web-Anwendung benutzt.

Inhalt

- *Verwalten von McAfee Advanced Threat Defense-Benutzern*
- *Überwachen der McAfee Advanced Threat Defense-Leistung*
- *Upgrade von McAfee Advanced Threat Defense und Android-VM*
- *Fehlerbehebung*
- *Sichern und Wiederherstellen der Advanced Threat Defense-Datenbank*

Verwalten von McAfee Advanced Threat Defense-Benutzern

Bei den Benutzerkonten für McAfee Advanced Threat Defense sind unterschiedliche Berechtigungen und Konfigurationseinstellungen möglich. Die Berechtigungen hängen von der Rolle ab, die ein Benutzer bei der Malware-Analyse mit McAfee Advanced Threat Defense spielt. Mithilfe der McAfee Advanced Threat Defense-Web-Anwendung können Sie Konten für folgende Benutzertypen erstellen:

- Benutzer, die die McAfee Advanced Threat Defense-Web-Anwendung zum Senden von Dateien zur Analyse und zum Anzeigen der Analyseergebnisse verwenden
- Benutzer, die die Dateien auf den FTP-Server hochladen, der auf der McAfee Advanced Threat Defense Appliance gehostet wird
- Benutzer, die zum Hochladen von Dateien direkt die REST-APIs benutzen. Weitere Informationen hierzu finden Sie im *McAfee Advanced Threat Defense RESTful APIs Reference Guide* (Referenzhandbuch zu McAfee Advanced Threat Defense-REST-APIs).

Sie können im Benutzerdatensatz auch das Standard-Analyseprofil festlegen. Wenn Sie für das Hochladen die McAfee Advanced Threat Defense-Web-Anwendung benutzen, können Sie diese Auswahl beim Datei-Upload außer Kraft setzen.

Sie können auch für jeden Benutzer die Details für den FTP-Server festlegen, auf den McAfee Advanced Threat Defense die Analyseergebnisse hochladen soll.

- Es stehen fünf Standard-Benutzerdatensätze zur Wahl.
  - Default Admin (Standard-Admin) – Dies ist das Standardbenutzerkonto für den Superuser. Mit diesem Konto können Sie anfänglich die McAfee Advanced Threat Defense-Web-Anwendung konfigurieren. Der Anmeldename lautet *admin*, und das Standardkennwort ist *admin*.
  - Network Security Platform – Der Anmeldename lautet *nsp*, und das Standardkennwort ist *admin*. Dies wird von Network Security Platform zur Integration in die McAfee Advanced Threat Defense verwendet.
  - ATD upload Admin (ATD-Upload-Admin) – Dies ist das Standardbenutzerkonto für den Zugriff auf den FTP-Server auf McAfee Advanced Threat Defense. Der Benutzername lautet *atdadmin*, und das Kennwort ist *adtadmin*.
  - McAfee Web Gateway – Dies dient der Integration von McAfee Web Gateway in McAfee Advanced Threat Defense.
  - McAfee Email Gateway – Dies dient der Integration von McAfee Email Gateway in McAfee Advanced Threat Defense.

  Aus Sicherheitsgründen sollten Sie die Standardkennwörter ändern.
- Für den Zugriff auf die McAfee Advanced Threat Defense-CLI müssen Sie *cliadmin* als Anmeldenamen und *atdadmin* als Kennwort verwenden. Auf diesen Benutzerdatensatz kann nicht zugegriffen werden. Sie können keinen anderen Benutzer zum Zugriff auf die CLI erstellen.

  Sie müssen über SSH und Port 2222 auf die CLI zugreifen. Siehe Anmelden über die Befehlszeilenschnittstelle (CLI) auf Seite 347.
- Wenn Sie kein Administratorbenutzer sind, können Sie auf Ihren Benutzerdatensatz zugreifen und ihn ändern. Zum Ändern Ihrer Rollenzuweisungen müssen Sie sich an den Administratorbenutzer wenden.

Anzeigen von Benutzerprofilen

Als Benutzer mit Administratorrolle können Sie die vorhandene Liste der McAfee Advanced Threat Defense-Benutzer anzeigen. Wenn Sie über keine Administratorrolle verfügen, können Sie nur Ihren eigenen Datensatz sehen.

Vorgehensweise

1 Wählen Sie **Verwalten** | **Benutzerverwaltung**.

Die aktuelle Liste der Benutzer wird angezeigt (abhängig von Ihrer Rolle).

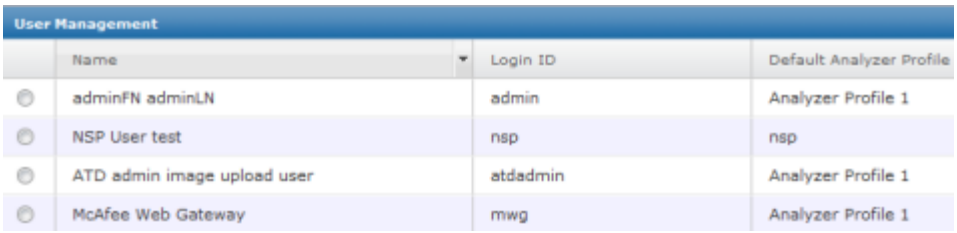


Abbildung 4-1 Angezeigte Benutzerliste

Spaltenname	Beschreibung
Auswählen	Dient zum Bearbeiten oder Löschen des Benutzerdatensatzes.
Name	Der vollständige Namen des Benutzers, wie in den Benutzerdetails angegeben.
Anmelde-ID	Der Benutzername für den Zugriff auf McAfee Advanced Threat Defense.
Default Analyzer Profile (Standard-Analyseprofil)	Das von McAfee Advanced Threat Defense verwendete Analyseprofil, wenn ein Benutzer eine Probe zur Analyse sendet. Es kann jedoch beim Einsenden der Probe vom Benutzer außer Kraft gesetzt werden.

2 Blenden Sie die Spalten aus, die Sie nicht sehen möchten.

a Bewegen Sie den Mauszeiger über die rechte Ecke einer Spaltenüberschrift, und klicken Sie auf den Dropdown-Pfeil.

b Wählen Sie **Columns** (Spalten).

c Wählen Sie nur die erforderlichen Spaltennamen aus der Liste.

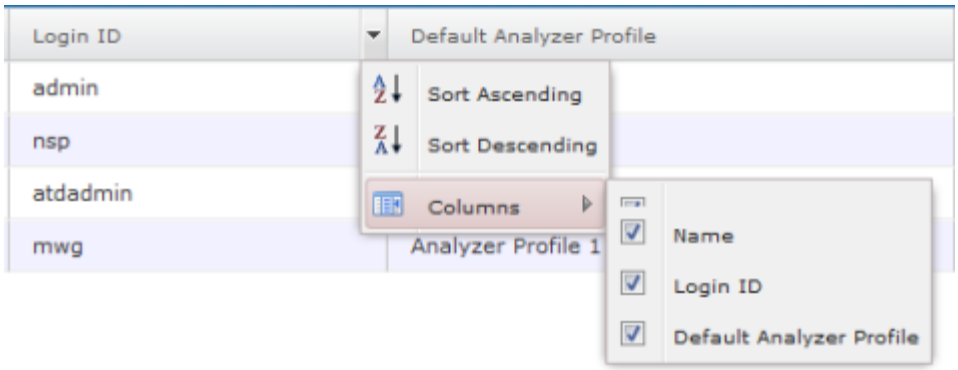


Abbildung 4-2 Auswählen der erforderlichen Spaltennamen

3 Zum Sortieren der Liste der Benutzerdatensätze basierend auf einem bestimmten Spaltennamen klicken Sie auf die Spaltenüberschrift.

Sie können die Datensätze in auf- oder absteigender Reihenfolge sortieren. Alternativ können Sie den Mauszeiger über die rechte Ecke einer Spaltenüberschrift bewegen und auf den Dropdown-Pfeil klicken. Wählen Sie dann **Sort Ascending** (Aufsteigend sortieren) oder **Sort Descending** (Absteigend sortieren).

4 Zum Anzeigen der vollständigen Details eines bestimmten Benutzers wählen Sie den Datensatz aus, und klicken Sie auf **Bearbeiten**.

Hinzufügen von Benutzern

Wenn Sie über die Rolle *Administratorbenutzer* verfügen, können Sie folgende Benutzertypen erstellen:

- Benutzer mit Administratorrolle in der McAfee Advanced Threat Defense-Web-Anwendung
- Nicht-Administratorbenutzer in der McAfee Advanced Threat Defense-Web-Anwendung
- Benutzer mit Zugriffsberechtigung für den FTP-Server auf der McAfee Advanced Threat Defense Appliance
- Benutzer mit Zugriffsberechtigung für die REST-APIs der McAfee Advanced Threat Defense-Web-Anwendung

Vorgehensweise

1 Wählen Sie **Verwalten** | **Benutzerverwaltung** | **Neu**.

Die Seite **Benutzerverwaltung** wird angezeigt.

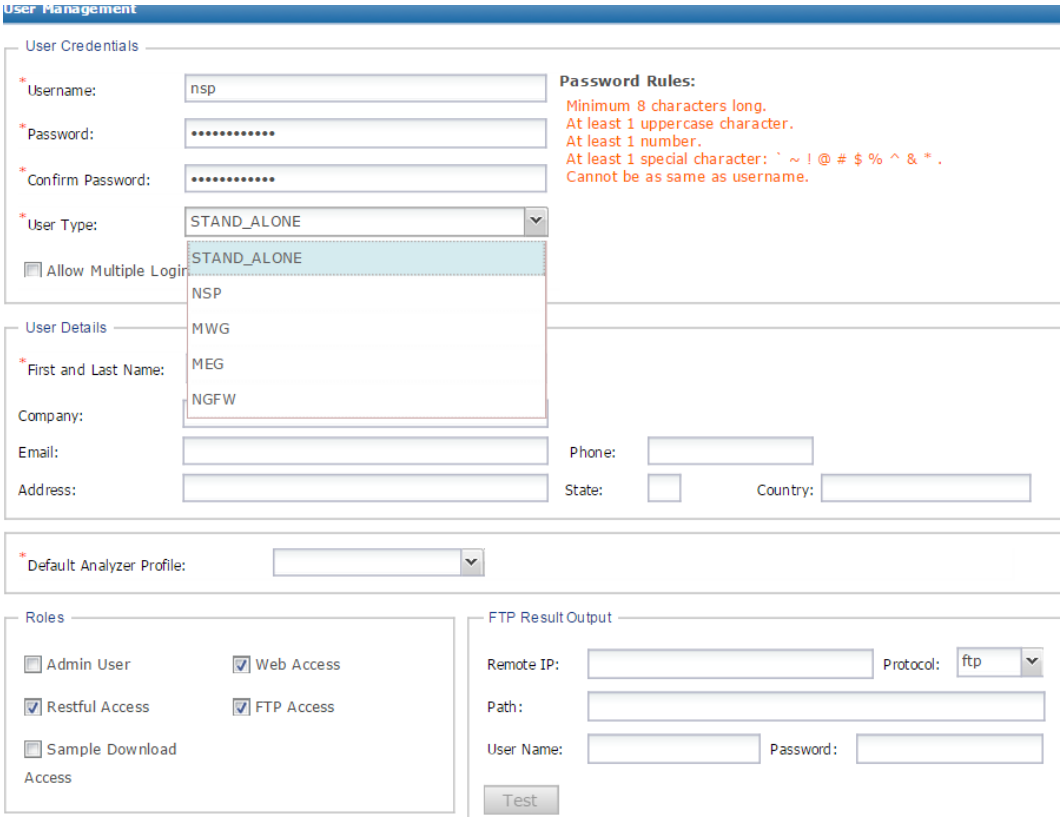


Abbildung 4-3 Hinzufügen von Benutzern

2 Geben Sie die entsprechenden Informationen in die jeweiligen Felder ein.

Optionsname	Beschreibung
Benutzername	Dies ist der Benutzername für den Zugriff auf die McAfee Advanced Threat Defense-Web-Anwendung, den FTP-Server oder die REST-APIs.
Kennwort	Dies ist das Standardkennwort, das Sie dem Benutzer zuweisen möchten. Es muss folgende Kriterien erfüllen: • Mindestens 8 Zeichen • Mindestens ein Großbuchstabe • Mindestens 1 Ziffer • Mindestens eines der folgenden Sonderzeichen: ` ~ ! @ # $ % ^ & * • Kennwort und Benutzername dürfen nicht übereinstimmen.
Allow Multiple Logins (Mehrere Anmeldungen zulassen)	Deaktivieren Sie diese Option, wenn Sie nur eine Anmeldesitzung für diesen Benutzernamen zulassen möchten. Aktivieren Sie die Option, um für den Benutzernamen mehrere gleichzeitige Anmeldungen zuzulassen.
First and Last Name (Vor- und Nachname)	Geben Sie den vollständigen Namen des Benutzers an. Er muss aus mindestens 2 Zeichen bestehen.
Email (E-Mail-Adresse)	Geben Sie optional die E-Mail-Adresse des Benutzers an.
Company (Unternehmen)	Geben Sie optional das Unternehmen an, dem der Benutzer angehört.
Telefon	Geben Sie optional die Telefonnummer des Benutzers an.
Anschrift	Geben Sie optional die Anschrift des Benutzers zu Kommunikationszwecken an.
State (Bundesland)	Geben Sie optional das der eingegebenen Anschrift entsprechende Bundesland an.
Land	Geben Sie optional das der eingegebenen Anschrift entsprechende Land an.
Default Analyzer Profile (Standard-Analyseprofil)	Wählen Sie das Analyseprofil für alle Dateien aus, die vom Benutzer gesendet werden. Benutzer, die Dateien manuell senden, können diese Einstellung außer Kraft setzen und für die Dateiübertragung ein anderes Analyseprofil auswählen.
Benutzertyp	Wählen Sie in der Dropdown-Liste einen Benutzertyp aus. Wählen Sie beispielsweise NSP aus, wenn Sie Proben mithilfe des Network Security Platform-Sensors senden möchten.

Optionsname	Beschreibung
Rollen	• **Admin User** (Administratorbenutzer) – Mit dieser Rolle können Sie Superuser-Rechte in derMcAfee Advanced Threat Defense-Web-Anwendung zuweisen. Benutzer mit dieser Rolle können auf alle Menüs zugreifen und andere Benutzer erstellen. • **Web Access** (Web-Zugriff) – Mit dieser Rolle kann ein Benutzer Dateien über die McAfee Advanced Threat Defense-Web-Anwendung senden und die Ergebnisse anzeigen. Benutzer mit dieser Rolle können auf alle Funktionen zugreifen, aber nur ihr eigenes Benutzerprofil anzeigen. Beim manuellen Senden von Dateien können sie nur das Analyseprofil zuweisen, das sie erstellt haben. • **FTP Access** (FTP-Zugriff) – Mit dieser Rolle haben Sie die Zugriffsberechtigung für den FTP-Server auf der McAfee Advanced Threat Defense Appliance, um Dateien für die Analyse zu senden und VMDK-Dateien hochzuladen. • **Log User Activities** (Benutzeraktivitäten protokollieren) – Wählen Sie diese Rolle aus, wenn Sie von Benutzern vorgenommene Änderungen in der McAfee Advanced Threat Defense-Web-Anwendung protokollieren möchten. • **Restful Access** (REST-Zugriff) – Mit dieser Rolle weisen Sie die Zugriffsberechtigung für REST-APIs der McAfee Advanced Threat Defense-Web-Anwendung zu, um Dateien für die Analyse zu senden. Für die integrierten McAfee-Produkte, die REST-APIs verwenden, muss die **Restful Access**-Rolle (REST-Zugriff) ausgewählt werden. Wenn Sie die Option deaktivieren, könnte die Integration fehlschlagen. • **Sample Download Access** (Zugriff auf Proben-Download) – Mit dieser Rolle kann ein Benutzer zuvor gesendete Proben herunterladen.

Optionsname	Beschreibung
FTP Result Output (FTP-Ergebnisausgabe)	Geben Sie die Details des FTP-Servers an, an den McAfee Advanced Threat Defense die Ergebnisse der Malware-Analyse senden soll. Wenn Sie die Details für den FTP-Server konfigurieren, sendet McAfee Advanced Threat Defense die Ergebnisse an den angegebenen FTP-Server und speichert diese im Datenspeicher. Sobald der Datenspeicher zu 75 % voll ist, werden die älteren Analyseergebnisse gelöscht. Um die Ergebnisse für einen längeren Zeitraum aufzubewahren, können Sie die **FTP Result Output** (FTP-Ergebnisausgabe) konfigurieren. • **Remote IP** (Remote-IP) – Dies ist die IPv4-Adresse des FTP-Servers. • **Protocol** (Protokoll) – Geben Sie an, ob FTP oder SFTP verwendet werden soll. McAfee empfiehlt die Verwendung von SFTP. • **Path** (Pfad) – Dies ist der vollständige Pfad zu dem Ordner, in dem die Ergebnisse gespeichert werden sollen. • **User Name** (Benutzername) – Dies ist der Benutzername, den McAfee Advanced Threat Defense verwenden soll, um auf den FTP-Server zuzugreifen. • **Kennwort** – Dies ist das Kennwort für den Zugriff auf den FTP-Server. • **Test** – Damit können Sie überprüfen, ob McAfee Advanced Threat Defense mithilfe des angegebenen Protokolls (FTP bzw. SFTP) mit dem angegebenen FTP-Server kommunizieren kann.
Speichern	Mit diesem Befehl wird der Benutzerdatensatz mit den angegebenen Informationen erstellt. Stellen Sie sicher, dass bei der Konfiguration des FTP-Servers für die Ergebnisausgabe die Testverbindung erfolgreich hergestellt werden konnte, bevor Sie auf **Speichern** klicken.
Abbrechen	Mit diesem Befehl wird die Seite **Benutzerverwaltung** ohne Speichern der Änderungen geschlossen.

Bearbeiten von Benutzern

Wenn Ihnen die Administratorbenutzerrolle zugewiesen ist, können Sie die Benutzerprofile bearbeiten. Falls Sie die Pflichtfelder ändern möchten, sollten Sie sicherstellen, dass der entsprechende Benutzer nicht angemeldet ist. Wenn Ihnen nur die Web-Zugriffs- oder REST-Zugriffsrolle zugewiesen ist, können Sie nur Ihr eigenes Benutzerprofil bearbeiten.

Vorgehensweise

1 Wählen Sie **Verwalten** | **Benutzerverwaltung**.

Die aktuelle Liste der Benutzer wird angezeigt.

2 Wählen Sie den gewünschten Benutzerdatensatz aus, und klicken Sie auf **Bearbeiten**.

Die Seite **Benutzerverwaltung** wird angezeigt.

3 Nehmen Sie die Änderungen an den gewünschten Feldern vor, und klicken Sie auf **Speichern**.

Informationen zu den Feldern finden Sie unter Hinzufügen von Benutzern auf Seite 40.

Löschen von Benutzern

Wenn Ihnen die Administratorbenutzerrolle zugewiesen ist, können Sie Benutzerdatensätze löschen. Vergewissern Sie sich, dass der entsprechende Benutzer nicht angemeldet ist.

Sie können keine vordefinierten Benutzerdatensätze löschen. Dazu gehören die Benutzerdatensätze für den Administrator, für Network Security Platform und für McAfee Web Gateway.

Vorgehensweise

1 Wählen Sie **Verwalten** | **Benutzerverwaltung**.

Die aktuelle Liste der Benutzer wird angezeigt.

2 Wählen Sie den gewünschten Benutzerdatensatz aus, und klicken Sie auf **Löschen**.

3 Klicken Sie auf **Ja**, um das Löschen zu bestätigen.

Überwachen der McAfee Advanced Threat Defense-Leistung

Die folgenden Optionen zur Überwachung der Leistung von McAfee Advanced Threat Defense sind verfügbar:

- Verwenden Sie die Monitore im McAfee Advanced Threat Defense-Dashboard, um die Leistung laufend zu überwachen. Siehe McAfee Advanced Threat Defense-Leistungsmonitore auf Seite 317.
- Verwenden Sie den Befehl `status` in der McAfee Advanced Threat Defense Appliance-CLI. Siehe CLI-Befehle für McAfee Advanced Threat Defense auf Seite 5.

Upgrade von McAfee Advanced Threat Defense und Android-VM

Dieser Abschnitt enthält Informationen zum Upgrade der McAfee Advanced Threat Defense-Version und der Android-Version für die standardmäßige Android-Analyse-VM.

Es folgen die Upgrade-Pfade für ein Upgrade der McAfee Advanced Threat Defense-Software auf 3.2.0.xx:

- Falls die aktuelle Version 3.0.2.xx und nicht 3.0.2.36 ist, wird ein direktes Upgrade auf 3.2.0.xx nicht unterstützt. Beispiel: Lautet die aktuelle Version 3.0.2.51, so aktualisieren Sie zuerst auf 3.0.4.56 und dann auf 3.2.0.xx. Das Upgrade von 3.0.2.xx auf 3.0.4.56 erfolgt als zweistufiger Prozess. Siehe Upgrade der McAfee Advanced Threat Defense-Software von 3.0.2.xx auf 3.0.4.xx auf Seite 45.
- Wenn die aktuelle Version 3.0.2.36 lautet und Sie ein Upgrade auf 3.2.0.xx durchführen möchten, aktualisieren Sie die McAfee Advanced Threat Defense-Benutzeroberfläche und die McAfee Advanced Threat Defense-Sytemsoftware separat. Das heißt, das direkte Upgrade auf 3.2.0 wird unterstützt, es erfolgt aber als zweistufiger Prozess. Siehe Upgrade der McAfee Advanced Threat Defense-Software von 3.0.2.36 auf 3.2.0.xx auf Seite 48.
- Lautet die aktuelle Version 3.0.4.56, 3.0.4.75 oder 3.0.4.94, können Sie ein direktes Upgrade auf 3.2.0.xx durchführen, indem Sie nur die McAfee Advanced Threat Defense-Systemsoftware aktualisieren. Siehe Upgrade der McAfee Advanced Threat Defense-Software von 3.0.4.xx auf 3.2.0.xx auf Seite 51.

Nach dem Upgrade auf 3.2.0.xx können Sie nicht mehr auf 3.0.2.xx oder auf 3.0.4.xx herunterstufen, indem Sie das Sicherungsabbild mit dem Befehl `reboot backup` laden.

- Lautet die aktuelle Version 3.2.0.xx, können Sie ein direktes Upgrade auf 3.2.2.xx durchführen, indem Sie nur die McAfee Advanced Threat Defense-Systemsoftware aktualisieren. Siehe Upgrade der ATD-Software von 3.2.0.xx auf 3.2.2.xx auf Seite 53.



Nach dem Upgrade auf 3.2.2.xx können Sie nicht mehr auf 3.0.2.xx, auf 3.0.4.xx oder auf 3.2.0.xx herunterstufen, indem Sie das Sicherungsabbild mit dem Befehl `reboot backup` laden.

Die Android-Version in der standardmäßigen Android-Analyse-VM lautet 2.3. Nach dem Upgrade der McAfee Advanced Threat Defense-Software auf 3.2.0.xx können Sie die Android-Version auf 4.3 aktualisieren. Siehe Upgrade der Android-Analyse-VM auf Seite 55.

Upgrade der McAfee Advanced Threat Defense-Software von 3.0.2.xx auf 3.0.4.xx

Bevor Sie beginnen

- Sie können ein Upgrade direkt auf 3.2.0 nur durchführen, wenn McAfee Advanced Threat Defense aktuell die Version 3.0.2.36 hat. Bei allen anderen 3.0.2.xx-Versionen müssen Sie, bevor Sie sie auf 3.2.0.xx aktualisieren können, zunächst ein Upgrade auf 3.0.4.56 durchführen.
- Vergewissern Sie sich, dass die McAfee Advanced Threat Defense-Software der Version 3.0.4.xx, die Sie verwenden möchten, extrahiert ist und Sie vom Client-Computer aus Zugriff darauf haben. Das Upgrade auf McAfee Advanced Threat Defense 3.0.4.56 erfolgt als zweistufiger Prozess. Sie aktualisieren die McAfee Advanced Threat Defense-Benutzeroberfläche und die McAfee Advanced Threat Defense-Systemsoftware separat. Stellen Sie daher sicher, dass Sie von Ihrem Client-Computer aus auf die Dateien *ui-3.0.4.X.msu* und *system-3.0.4.x.msu* zugreifen können.

  Dieser zweistufige Upgrade-Vorgang ist nur erforderlich, wenn Sie ein Upgrade von Version 3.0.2.x auf 3.0.4.56 durchführen. Bevor Sie die Version auf 3.0.4.75 aktualisieren können, müssen Sie zunächst ein Upgrade auf 3.0.4.56 durchführen. Um anschließend ein Upgrade von 3.0.4.56 auf 3.0.4.75 durchzuführen, müssen Sie lediglich die Benutzeroberfläche der McAfee Advanced Threat Defense-Web-Anwendung (MATD-Software) aktualisieren.
- Sie verfügen über die Anmeldeinformationen, um sich als Administratorbenutzer bei der McAfee Advanced Threat Defense-Web-Anwendung anzumelden.
- Sie verfügen über die Anmeldeinformationen, um sich mit SSH bei der McAfee Advanced Threat Defense-CLI anzumelden.
- Sie verfügen über die Anmeldeinformationen für das SFTP der McAfee Advanced Threat Defense Appliance.
- Für den *admin*-Benutzerdatensatz wählen Sie auf der Seite **Benutzerverwaltung** die Option **Allow Multiple Logins** (Mehrere Anmeldungen zulassen) aus.

Mithilfe der McAfee Advanced Threat Defense-Web-Anwendung können Sie das McAfee Advanced Threat Defense-Software-Image, auf das Sie aktualisieren möchten, importieren.



Starten Sie das Gerät vorsichtshalber von der aktiven Festplatte aus neu, und benutzen Sie den `copyto backup`-Befehl zum Kopieren der Softwareversion von der aktiven Festplatte auf die Sicherungsfestplatte. Dank der Sicherung können Sie bei Bedarf zur aktuellen Softwareversion zurückkehren.

Vorgehensweise

1 Führen Sie ein Upgrade der Benutzeroberfläche der McAfee Advanced Threat Defense-Web-Anwendung durch.

a Wählen Sie **Verwalten** | **Software-Verwaltung** aus.

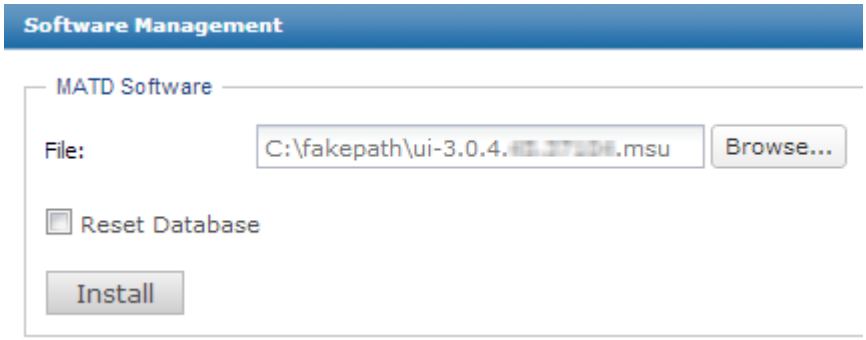


Abbildung 4-4 Upgrade der McAfee Advanced Threat Defense-Web-Anwendung

b Klicken Sie auf **Durchsuchen**, und wählen Sie die Datei "ui-<version number>.msu" auf Ihrem Client-Computer aus.

Wenn Sie ein Upgrade durchführen möchten, stellen Sie sicher, dass **Datenbank zurücksetzen** nicht ausgewählt ist. Sie wählen diese Option nur aus, wenn Sie im Laufe des Upgrades eine neue Datenbank erstellen möchten. Bei Auswahl dieser Option wird eine Warnung angezeigt, dass alle Daten der vorhandenen Datenbank verloren gehen. Klicken Sie zur Bestätigung auf **OK**.

c Klicken Sie auf **Installieren**.

d Melden Sie sich nach dem Upgrade der McAfee Advanced Threat Defense-Web-Anwendung ab, und löschen Sie den Cache des verwendeten Browsers.

e Melden Sie sich bei der McAfee Advanced Threat Defense-Web-Anwendung an, und führen Sie folgende Schritte aus.

- Überprüfen Sie die in der Benutzeroberfläche angezeigte Version.
- Wählen Sie **Verwalten** | **Software-Verwaltung** aus, und überprüfen Sie, ob sich die **Software-Verwaltung** aus zwei Abschnitten – MATD-Software und Systemsoftware – zusammensetzt.
- Stellen Sie sicher, dass die Daten und Konfigurationen Ihrer früheren Version übernommen wurden.

2 Führen Sie ein Upgrade der McAfee Advanced Threat Defense-Systemsoftware durch.

a Melden Sie sich mithilfe eines FTP-Clients wie FileZilla bei der McAfee Advanced Threat Defense Appliance an.

Melden Sie sich als der Benutzer "atdadmin" an.

b Laden Sie die Datei "system-<version number>.msu" über SFTP in das Stammverzeichnis von McAfee Advanced Threat Defense hoch.

Stellen Sie sicher, dass die Übertragung im Binärmodus erfolgt.

c Melden Sie sich nach dem Hochladen der Datei als Administratorbenutzer bei der McAfee Advanced Threat Defense-Web-Anwendung an, und wählen Sie **Verwalten** | **Software-Verwaltung**.

d Wählen Sie unter **System Software** (Systemsoftware) die Datei "system-<version number>.msu" aus.

e Stellen Sie für den Fall von Upgrades sicher, dass **Datenbank zurücksetzen** nicht ausgewählt ist, und klicken Sie auf **Installieren**.

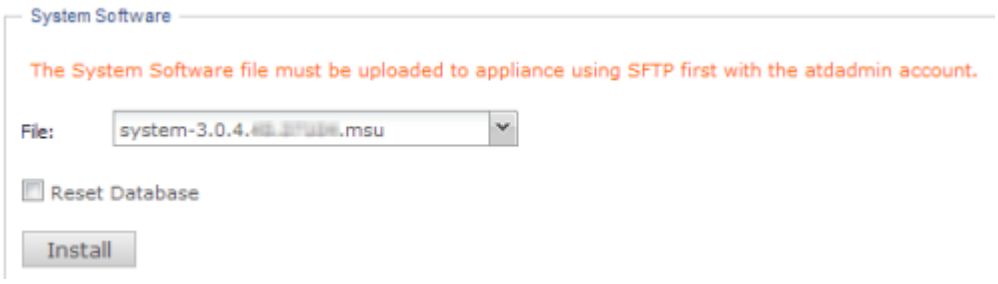
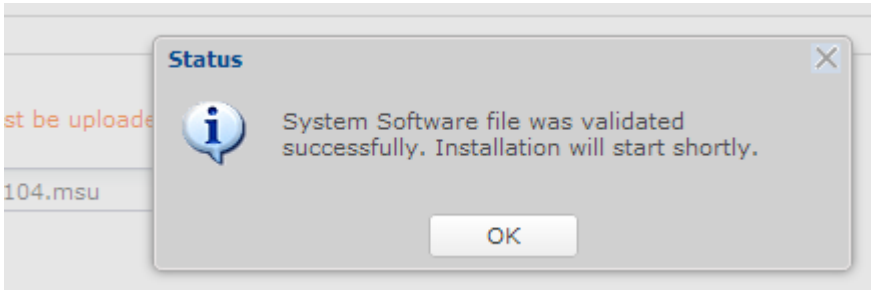
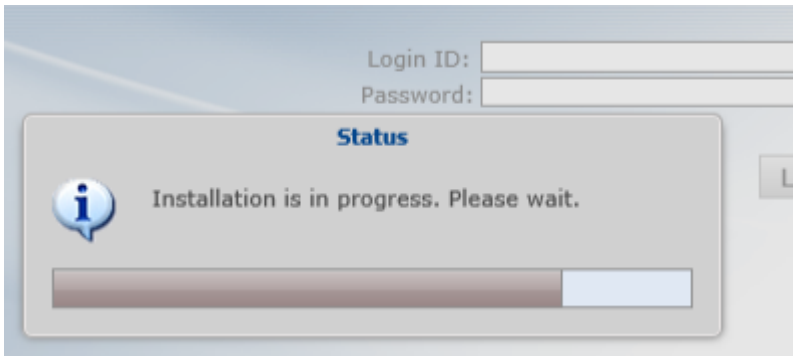


Abbildung 4-5 Upgrade der McAfee Advanced Threat Defense-Web-Anwendung

f Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **OK**.



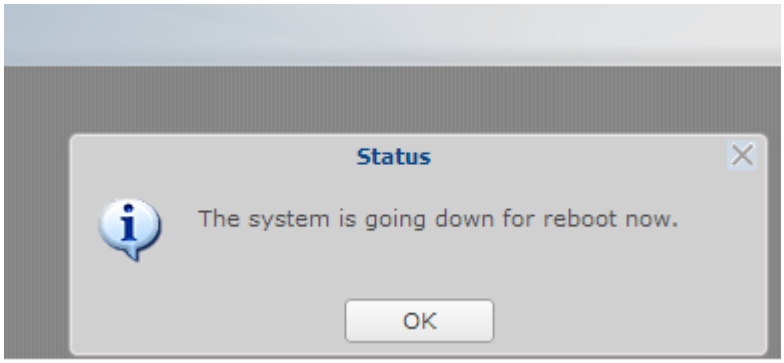
Die Systemsoftware wird installiert, und der Status wird im Browser angezeigt.



Die Installation der Systemsoftware dauert mindestens 20 Minuten.

g Nachdem die Software installiert wurde, startet die McAfee Advanced Threat Defense Appliance neu. Eine entsprechende Meldung wird angezeigt.

Die Appliance startet eigenständig neu. Die angezeigte Meldung dient nur zu Ihrer Information.



Wenn Sie diese Meldungen nicht sehen können, löschen Sie den Browser-Cache.

h Warten Sie, bis die McAfee Advanced Threat Defense Appliance gestartet wurde. Melden Sie sich bei der CLI an, und überprüfen Sie die Softwareversion.

i Überprüfen Sie die Version in der McAfee Advanced Threat Defense-Web-Anwendung.

j Melden Sie sich bei der Web-Anwendung an, und überprüfen Sie auf der Seite **Systemprotokoll**, ob die vmcreator-Task aufgerufen wurde.

Wenn Sie ein Upgrade auf McAfee Advanced Threat Defense 3.0.4 durchführen, werden alle Analyse-VMs automatisch neu erstellt. Dieser Prozess nimmt je nach Anzahl der Analyse-VMs etwas Zeit in Anspruch.

k Stellen Sie sicher, dass die Daten und Konfigurationen Ihrer früheren Version übernommen wurden.

Die aktualisierte Softwareversion ist jetzt auf der aktiven Festplatte der McAfee Advanced Threat Defense Appliance gespeichert.

Upgrade der McAfee Advanced Threat Defense-Software von 3.0.2.36 auf 3.2.0.xx

Bevor Sie beginnen

- Sie können ein Upgrade direkt auf 3.2.0 nur durchführen, wenn McAfee Advanced Threat Defense aktuell die Version 3.0.2.36 hat. Bei allen anderen 3.0.2.xx-Versionen müssen Sie, bevor Sie sie auf 3.2.0.xx aktualisieren können, zunächst ein Upgrade auf 3.0.4.56 durchführen.
- Vergewissern Sie sich, dass die McAfee Advanced Threat Defense-Software der Version 3.2.0.xx, die Sie verwenden möchten, extrahiert ist und Sie vom Client-Computer aus Zugriff darauf haben. Das Upgrade auf McAfee Advanced Threat Defense 3.2.0.xx erfolgt als zweistufiger Prozess. Sie aktualisieren die McAfee Advanced Threat Defense-Benutzeroberfläche und die McAfee Advanced Threat Defense-Systemsoftware separat. Stellen Sie daher sicher, dass Sie von Ihrem Client-Computer aus auf die Dateien *ui-3.2.0.X.msu* und *system-3.2.0.x.msu* zugreifen können.
- Sie verfügen über die Anmeldeinformationen, um sich als Administratorbenutzer bei der McAfee Advanced Threat Defense-Web-Anwendung anzumelden.

- Sie verfügen über die Anmeldeinformationen, um sich mit SSH bei der McAfee Advanced Threat Defense-CLI anzumelden.
- Sie verfügen über die Anmeldeinformationen für das SFTP der McAfee Advanced Threat Defense Appliance.
- Für den *admin*-Benutzerdatensatz wählen Sie auf der Seite **Benutzerverwaltung** die Option **Allow Multiple Logins** (Mehrere Anmeldungen zulassen) aus.

Mithilfe der McAfee Advanced Threat Defense-Web-Anwendung können Sie das McAfee Advanced Threat Defense-Software-Image, auf das Sie aktualisieren möchten, importieren.

Vorgehensweise

1 Führen Sie ein Upgrade der Benutzeroberfläche der McAfee Advanced Threat Defense-Web-Anwendung durch.

a Wählen Sie **Verwalten** | **Software-Verwaltung** aus.

b Klicken Sie auf **Durchsuchen**, und wählen Sie die Datei "ui-3.2.0.X.msu" auf Ihrem Client-Computer aus.



Wenn Sie ein Upgrade durchführen möchten, stellen Sie sicher, dass **Datenbank zurücksetzen** nicht ausgewählt ist. Sie wählen diese Option nur aus, wenn Sie im Laufe des Upgrades eine neue Datenbank erstellen möchten. Bei Auswahl dieser Option wird eine Warnung angezeigt, dass alle Daten der vorhandenen Datenbank verloren gehen. Klicken Sie zur Bestätigung auf **OK**.

c Klicken Sie auf **Installieren**.

d Melden Sie sich nach dem Upgrade der McAfee Advanced Threat Defense-Web-Anwendung ab, und löschen Sie den Cache des verwendeten Browsers.

e Melden Sie sich bei der McAfee Advanced Threat Defense-Web-Anwendung an, und führen Sie folgende Schritte aus.

- Überprüfen Sie die in der Benutzeroberfläche angezeigte Version.
- Wählen Sie **Verwalten** | **Software-Verwaltung** aus, und überprüfen Sie, ob sich die **Software-Verwaltung** aus zwei Abschnitten – **MATD-Software** und **Systemsoftware** – zusammensetzt.
- Stellen Sie sicher, dass die Daten und Konfigurationen Ihrer früheren Version übernommen wurden.

2 Führen Sie ein Upgrade der McAfee Advanced Threat Defense-Systemsoftware durch.

a Melden Sie sich mithilfe eines FTP-Clients wie FileZilla bei der McAfee Advanced Threat Defense Appliance an.

Melden Sie sich als der Benutzer "atdadmin" an.

b Laden Sie die Datei "system-3.2.0.x.msu" über SFTP in das Stammverzeichnis von McAfee Advanced Threat Defense hoch.



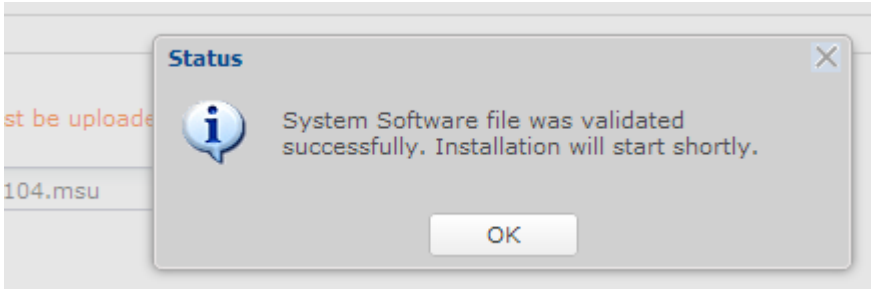
Stellen Sie sicher, dass die Übertragung im Binärmodus erfolgt.

c Melden Sie sich nach dem Hochladen der Datei als Administratorbenutzer bei der McAfee Advanced Threat Defense-Web-Anwendung an, und wählen Sie **Verwalten** | **Software-Verwaltung**.

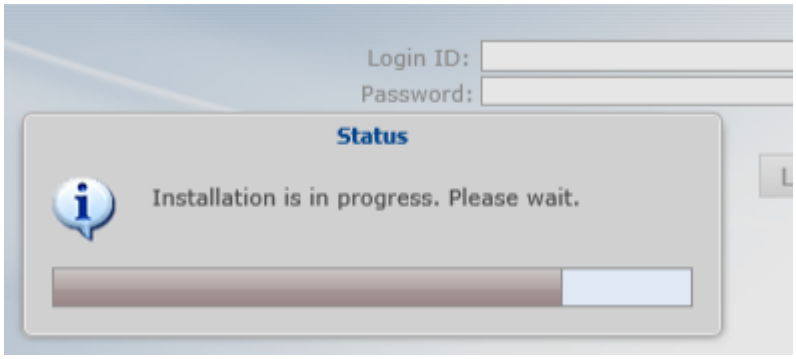
d Wählen Sie unter **System Software** (Systemsoftware) die Datei "system-3.2.0.x.msu" aus.

e Stellen Sie für den Fall von Upgrades sicher, dass **Datenbank zurücksetzen** nicht ausgewählt ist, und klicken Sie auf **Installieren**.

f Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **OK**.



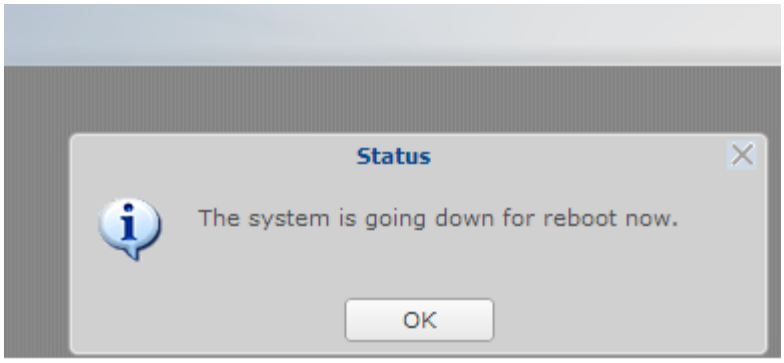
Die Systemsoftware wird installiert, und der Status wird im Browser angezeigt.



Die Installation der Systemsoftware dauert mindestens 20 Minuten.

g Nachdem die Software installiert wurde, startet die McAfee Advanced Threat Defense Appliance neu. Eine entsprechende Meldung wird angezeigt.

Die Appliance startet eigenständig neu. Die angezeigte Meldung dient nur zu Ihrer Information.



Wenn Sie diese Meldungen nicht sehen können, löschen Sie den Browser-Cache.

h Warten Sie, bis die McAfee Advanced Threat Defense Appliance gestartet wurde. Melden Sie sich bei der CLI an, und überprüfen Sie die Softwareversion.

i Überprüfen Sie die Version in der McAfee Advanced Threat Defense-Web-Anwendung.

j Melden Sie sich bei der Web-Anwendung an, und überprüfen Sie auf der Seite **Systemprotokoll**, ob die vmcreator-Task aufgerufen wurde.



Wenn Sie ein Upgrade auf McAfee Advanced Threat Defense 3.2.0 durchführen, werden alle Analyse-VMs automatisch neu erstellt. Dieser Prozess nimmt je nach Anzahl der Analyse-VMs etwas Zeit in Anspruch.

k Stellen Sie sicher, dass die Daten und Konfigurationen Ihrer früheren Version übernommen wurden.

Die aktualisierte Softwareversion ist jetzt auf der aktiven Festplatte der McAfee Advanced Threat Defense Appliance gespeichert.

Upgrade der McAfee Advanced Threat Defense-Software von 3.0.4.xx auf 3.2.0.xx

Bevor Sie beginnen

- Stellen Sie sicher, dass die aktuelle McAfee Advanced Threat Defense-Version 3.0.4.56, 3.0.75 oder 3.0.4.94 lautet. Wenn die aktuelle Version 3.0.2.xx lautet, lesen Sie sich die Upgrade-Informationen im entsprechenden Abschnitt durch.
- Vergewissern Sie sich, dass die *system-3.2.0.x.msu* der McAfee Advanced Threat Defense-Software, die Sie verwenden möchten, extrahiert ist und Sie vom Client-Computer aus Zugriff darauf haben.
- Sie verfügen über die Anmeldeinformationen, um sich als Administratorbenutzer bei der McAfee Advanced Threat Defense-Web-Anwendung anzumelden.
- Sie verfügen über die Anmeldeinformationen, um sich mit SSH bei der McAfee Advanced Threat Defense-CLI anzumelden.
- Sie verfügen über die Anmeldeinformationen für das SFTP der McAfee Advanced Threat Defense Appliance.
- Für den *admin*-Benutzerdatensatz wählen Sie auf der Seite **Benutzerverwaltung** die Option **Allow Multiple Logins** (Mehrere Anmeldungen zulassen) aus.

Mithilfe der McAfee Advanced Threat Defense-Web-Anwendung können Sie das McAfee Advanced Threat Defense-Software-Image, auf das Sie aktualisieren möchten, importieren.

Vorgehensweise

1 Melden Sie sich mithilfe eines FTP-Clients wie FileZilla bei der McAfee Advanced Threat Defense Appliance an.

Melden Sie sich als der Benutzer "atdadmin" an.

2 Laden Sie die Datei "system-<version number>.msu" über SFTP in das Stammverzeichnis von McAfee Advanced Threat Defense hoch.



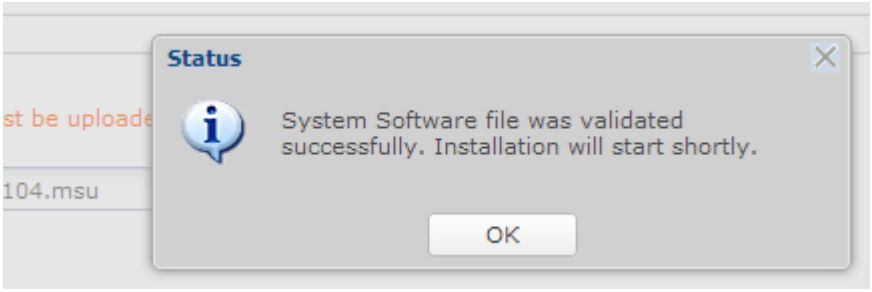
Stellen Sie sicher, dass die Übertragung im Binärmodus erfolgt.

3 Melden Sie sich nach dem Hochladen der Datei als Administratorbenutzer bei der McAfee Advanced Threat Defense-Web-Anwendung an, und wählen Sie **Verwalten** | **Software-Verwaltung**.

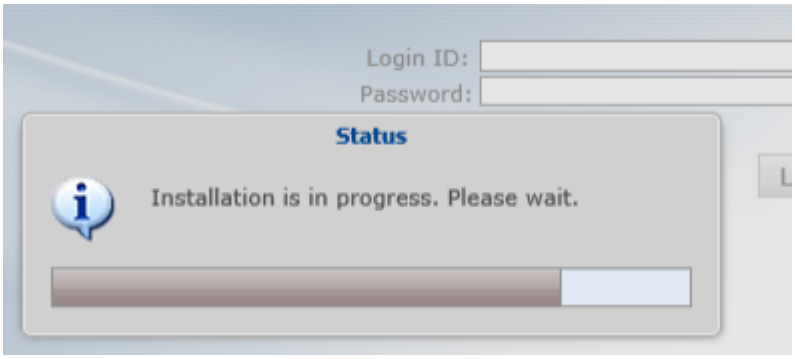
4 Wählen Sie unter **System Software** (Systemsoftware) die Datei "system-<version number>.msu" aus.

5 Stellen Sie für den Fall von Upgrades sicher, dass **Datenbank zurücksetzen** nicht ausgewählt ist, und klicken Sie auf **Installieren**.

6 Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **OK**.



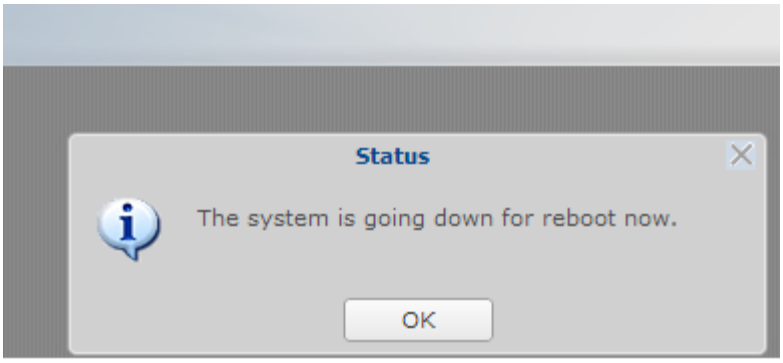
Die Systemsoftware wird installiert, und der Status wird im Browser angezeigt.



Die Installation der Systemsoftware dauert mindestens 20 Minuten.

7 Nachdem die Software installiert wurde, startet die McAfee Advanced Threat Defense Appliance neu. Eine entsprechende Meldung wird angezeigt.

Die Appliance startet eigenständig neu. Die angezeigte Meldung dient nur zu Ihrer Information.



Wenn Sie diese Meldungen nicht sehen können, löschen Sie den Browser-Cache.

8 Warten Sie, bis die McAfee Advanced Threat Defense Appliance gestartet wurde. Melden Sie sich bei der CLI an, und überprüfen Sie die Softwareversion.

9 Überprüfen Sie die Version in der McAfee Advanced Threat Defense-Web-Anwendung.

10 Melden Sie sich bei der Web-Anwendung an, und überprüfen Sie auf der Seite **Systemprotokoll**, ob die vmcreator-Task aufgerufen wurde.



Wenn Sie ein Upgrade auf McAfee Advanced Threat Defense 3.2.0 durchführen, werden alle Analyse-VMs automatisch neu erstellt. Dieser Prozess nimmt je nach Anzahl der Analyse-VMs etwas Zeit in Anspruch.

11 Stellen Sie sicher, dass die Daten und Konfigurationen Ihrer früheren Version übernommen wurden.

Die aktualisierte Softwareversion ist jetzt auf der aktiven Festplatte der McAfee Advanced Threat Defense Appliance gespeichert.

Upgrade der ATD-Software von 3.2.0.xx auf 3.2.2.xx

Bevor Sie beginnen

- Stellen Sie sicher, dass die aktuelle McAfee Advanced Threat Defense-Version 3.2.0.xx lautet.
- Vergewissern Sie sich, dass die *system-3.2.2.x.msu* der McAfee Advanced Threat Defense-Software, die Sie verwenden möchten, extrahiert ist und Sie vom Client-Computer aus Zugriff darauf haben.
- Sie verfügen über die Anmeldeinformationen, um sich als Administratorbenutzer bei der McAfee Advanced Threat Defense-Web-Anwendung anzumelden.
- Sie verfügen über die Anmeldeinformationen, um sich mit SSH bei der McAfee Advanced Threat Defense-CLI anzumelden.
- Sie verfügen über die Anmeldeinformationen für das SFTP der McAfee Advanced Threat Defense Appliance.
- Für den *admin*-Benutzerdatensatz wählen Sie auf der Seite **Benutzerverwaltung** die Option **Allow Multiple Logins** (Mehrere Anmeldungen zulassen) aus.

Mithilfe der McAfee Advanced Threat Defense-Web-Anwendung können Sie das McAfee Advanced Threat Defense-Software-Image, auf das Sie aktualisieren möchten, importieren.

Vorgehensweise

1 Melden Sie sich mithilfe eines FTP-Clients wie FileZilla bei der McAfee Advanced Threat Defense Appliance an.

Melden Sie sich als der Benutzer "atdadmin" an.

2 Laden Sie die Datei "system-<version number>.msu" über SFTP in das Stammverzeichnis von McAfee Advanced Threat Defense hoch.



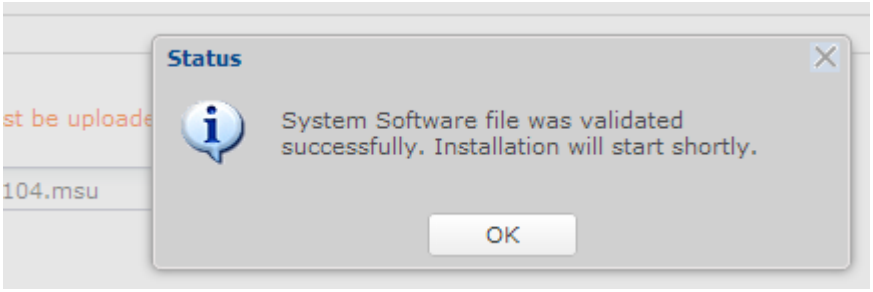
Stellen Sie sicher, dass die Übertragung im Binärmodus erfolgt.

3 Melden Sie sich nach dem Hochladen der Datei als Administratorbenutzer bei der McAfee Advanced Threat Defense-Web-Anwendung an, und wählen Sie **Verwalten** | **Software-Verwaltung**.

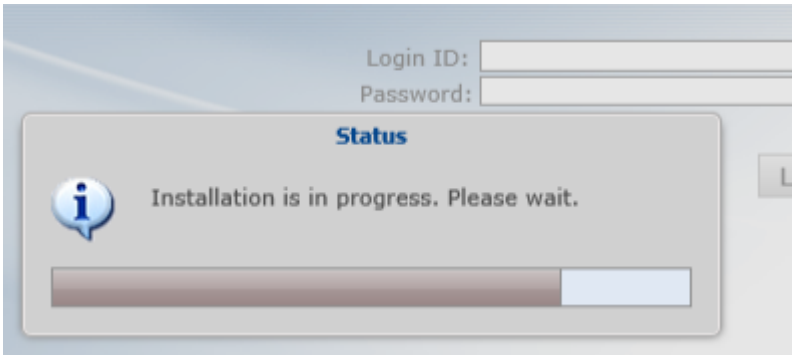
4 Wählen Sie unter **System Software** (Systemsoftware) die Datei "system-<version number>.msu" aus.

5 Stellen Sie für den Fall von Upgrades sicher, dass **Datenbank zurücksetzen** nicht ausgewählt ist, und klicken Sie auf **Installieren**.

6 Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **OK**.



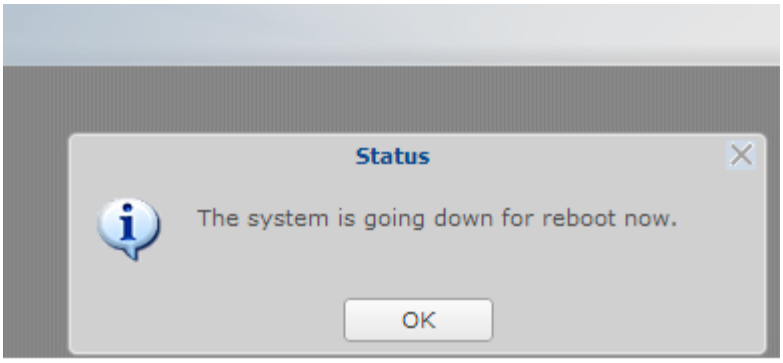
Die Systemsoftware wird installiert, und der Status wird im Browser angezeigt.



Die Installation der Systemsoftware dauert mindestens 20 Minuten.

7 Nachdem die Software installiert wurde, startet die McAfee Advanced Threat Defense Appliance neu. Eine entsprechende Meldung wird angezeigt.

Die Appliance startet eigenständig neu. Die angezeigte Meldung dient nur zu Ihrer Information.



Wenn Sie diese Meldungen nicht sehen können, löschen Sie den Browser-Cache.

8 Warten Sie, bis die McAfee Advanced Threat Defense Appliance gestartet wurde. Melden Sie sich bei der CLI an, und überprüfen Sie die Softwareversion.

9 Überprüfen Sie die Version in der McAfee Advanced Threat Defense-Web-Anwendung.

10 Melden Sie sich bei der Web-Anwendung an, und überprüfen Sie auf der Seite **Systemprotokoll**, ob die vmcreator-Task aufgerufen wurde.



Wenn Sie ein Upgrade auf McAfee Advanced Threat Defense 3.2.2 durchführen, werden alle Analyse-VMs automatisch neu erstellt. Dieser Prozess nimmt je nach Anzahl der Analyse-VMs etwas Zeit in Anspruch.

11 Stellen Sie sicher, dass die Daten und Konfigurationen Ihrer früheren Version übernommen wurden.

Die aktualisierte Softwareversion ist jetzt auf der aktiven Festplatte der McAfee Advanced Threat Defense Appliance gespeichert.

Upgrade der Android-Analyse-VM

Bevor Sie beginnen

- Stellen Sie sicher, dass die aktuelle McAfee Advanced Threat Defense-Version 3.2.0.xx lautet.
- Vergewissern Sie sich, dass die *android-4.3.msu* extrahiert ist und Sie vom Client-Computer aus Zugriff darauf haben.
- Sie verfügen über die Anmeldeinformationen, um sich als Administratorbenutzer bei der McAfee Advanced Threat Defense-Web-Anwendung anzumelden.
- Sie verfügen über die Anmeldeinformationen, um sich mit SSH bei der McAfee Advanced Threat Defense-CLI anzumelden.
- Sie verfügen über die Anmeldeinformationen für das SFTP der McAfee Advanced Threat Defense Appliance.
- Für den *admin*-Benutzerdatensatz wählen Sie auf der Seite **Benutzerverwaltung** die Option **Allow Multiple Logins** (Mehrere Anmeldungen zulassen) aus.

Mit der McAfee Advanced Threat Defense-Web-Anwendung können Sie ein Upgrade der Android-Analyse-VM auf Version 4.3 durchführen.

Vorgehensweise

1 Melden Sie sich mithilfe eines FTP-Clients wie FileZilla bei der McAfee Advanced Threat Defense Appliance an.

Melden Sie sich als der Benutzer "atdadmin" an.

2 Laden Sie die Datei *android-4.3.msu* über SFTP in das Stammverzeichnis von McAfee Advanced Threat Defense hoch.



Stellen Sie sicher, dass die Übertragung im Binärmodus erfolgt.

3 Melden Sie sich nach dem Hochladen der Datei als Administratorbenutzer bei der McAfee Advanced Threat Defense-Web-Anwendung an, und wählen Sie **Verwalten** | **Software-Verwaltung**.

4 Wählen Sie unter **System Software** (Systemsoftware) die Datei *android-4.3.msu* aus.

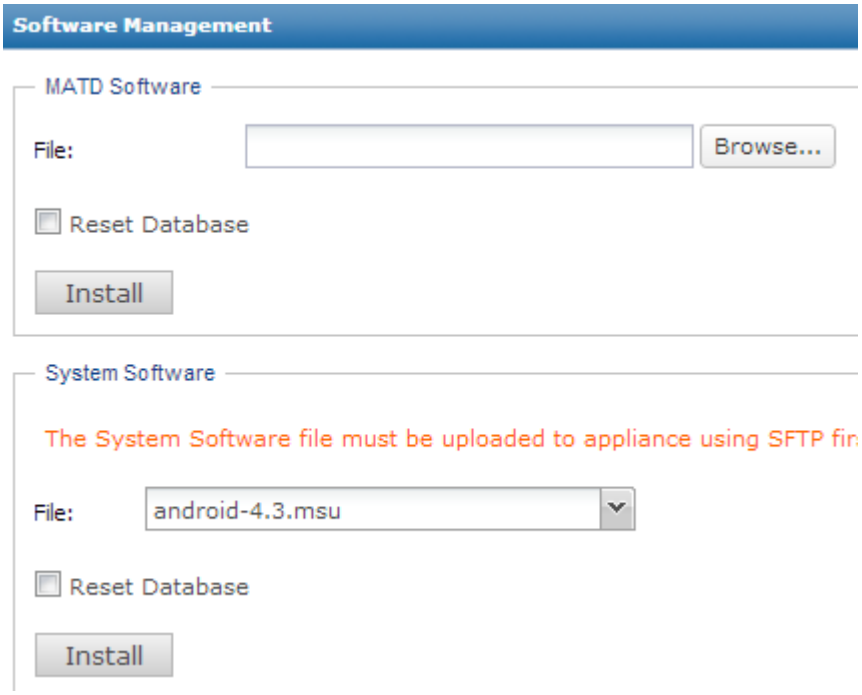
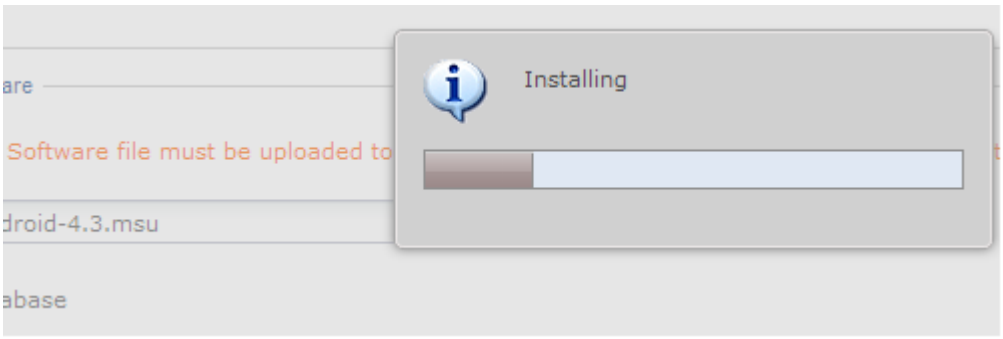


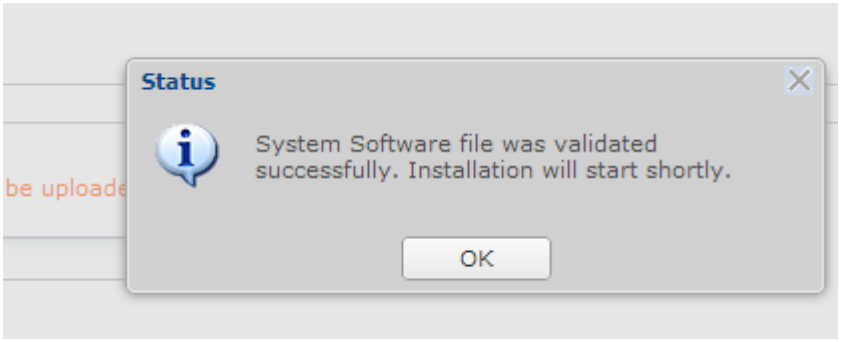
Abbildung 4-6 Auswählen der Android-Datei

5 Stellen Sie sicher, dass **Datenbank zurücksetzen** nicht ausgewählt ist, da diese Option für Android-Upgrades nicht relevant ist, und klicken Sie auf **Installieren**.

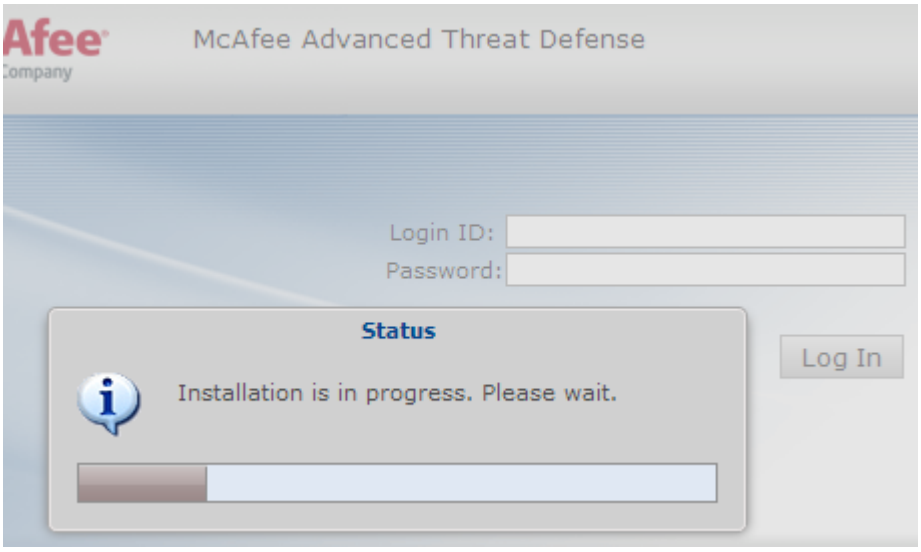
Die Android-Installation beginnt mit der Dateivalidierung.



6 Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **OK**.



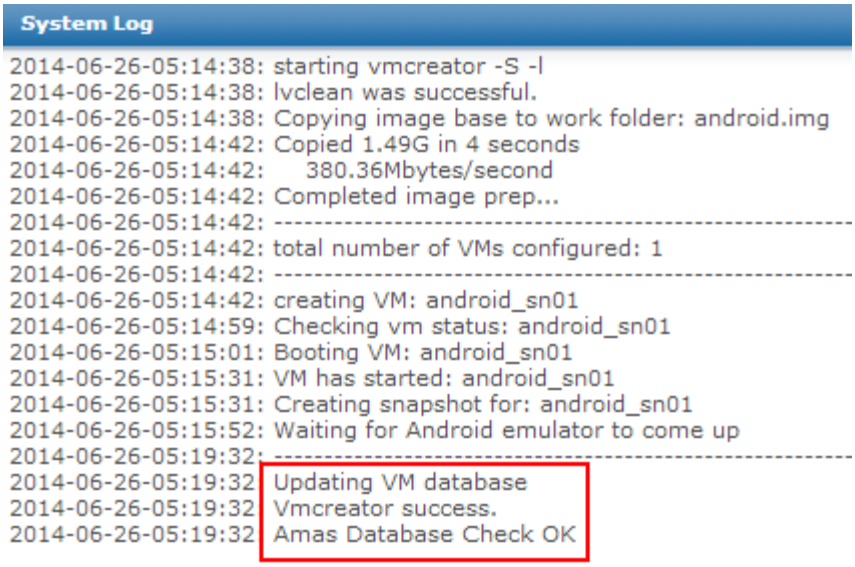
Die McAfee Advanced Threat Defense-Web-Anwendung wird automatisch geschlossen, und der Status der Installation wird im Browser angezeigt.



- Die Installation der Systemsoftware dauert mindestens 20 Minuten.
- Wenn Sie diese Meldungen nicht sehen können, löschen Sie den Browser-Cache.
- Wenn Sie ein Android-Upgrade durchführen, wird die standardmäßige Android-Analyse-VM automatisch neu erstellt. Dieser Vorgang kann einige Minuten dauern.

7 Melden Sie sich bei der Web-Anwendung an, und wählen Sie **Verwalten** | **Systemprotokoll** aus.

8 Prüfen Sie auf der Seite **Systemprotokoll**, ob die vmcreator-Task für die Android-Analyse-VM erfolgreich abgeschlossen wurde.


System Log
2014-06-26-05:14:38: starting vmcreator -S -l
2014-06-26-05:14:38: lvclean was successful.
2014-06-26-05:14:38: Copying image base to work folder: android.img
2014-06-26-05:14:42: Copied 1.49G in 4 seconds
2014-06-26-05:14:42: 380.36Mbytes/second
2014-06-26-05:14:42: Completed image prep...
2014-06-26-05:14:42: ----------
2014-06-26-05:14:42: total number of VMs configured: 1
2014-06-26-05:14:42: ----------
2014-06-26-05:14:42: creating VM: android_sn01
2014-06-26-05:14:59: Checking vm status: android_sn01
2014-06-26-05:15:01: Booting VM: android_sn01
2014-06-26-05:15:31: VM has started: android_sn01
2014-06-26-05:15:31: Creating snapshot for: android_sn01
2014-06-26-05:15:52: Waiting for Android emulator to come up
2014-06-26-05:19:32: ----------
2014-06-26-05:19:32 Updating VM database
2014-06-26-05:19:32 Vmcreator success.
2014-06-26-05:19:32 Amas Database Check OK

Fehlerbehebung

Auf der Seite **Troubleshooting** (Fehlerbehebung) können Sie einige Aufgaben zur Fehlerbehebung bei der McAfee Advanced Threat Defense-Web-Anwendung ausführen. Dazu zählen das Exportieren von Protokollen aus McAfee Advanced Threat Defense und das Löschen aller gespeicherten Analyseergebnisse aus der McAfee Advanced Threat Defense-Datenbank.

Vorgehensweise

- Um auf die Seite **Troubleshooting** (Fehlerbehebung) zuzugreifen, wählen Sie **Verwalten** | **Troubleshooting (Fehlerbehebung).**

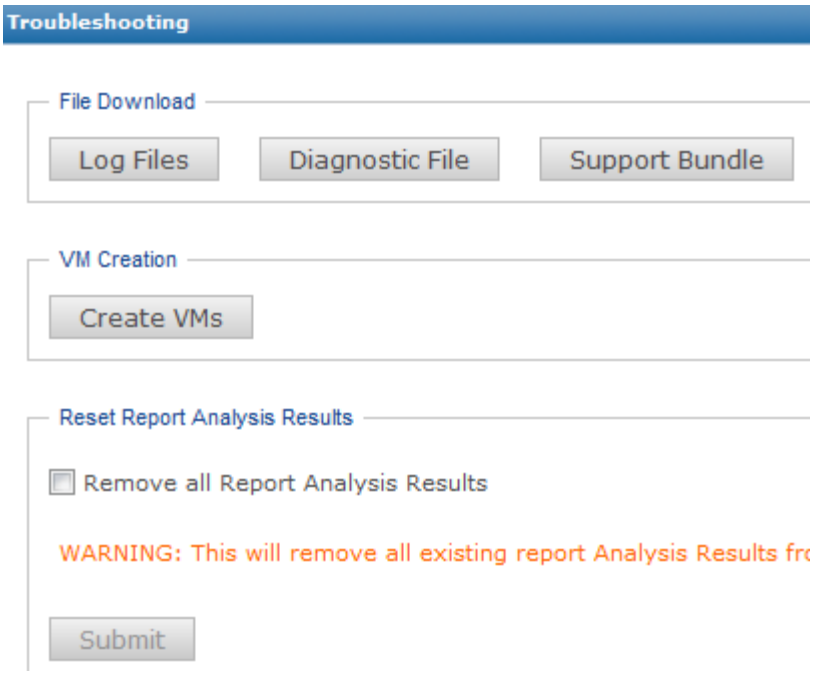


Abbildung 4-7 Seite "Troubleshooting" (Fehlerbehebung)

Aufgaben

- *Exportieren von McAfee Advanced Threat Defense-Protokollen* auf Seite 59
- *Neuerstellen der Analyse-VMs* auf Seite 60
- *Löschen der Analyseergebnisse* auf Seite 61

Exportieren von McAfee Advanced Threat Defense-Protokollen

Wenn Probleme mit McAfee Advanced Threat Defense auftreten, können Sie die Protokolldateien exportieren und zur Analyse und Fehlerbehebung an den McAfee-Support senden. Sie können Systemprotokolle, Diagnoseprotokolle und sonstige Protokolltypen exportieren. Die Systemprotokolle helfen bei der Behebung von Fehlern, die im Zusammenhang mit Funktionen, Vorgängen, Ereignissen und so weiter stehen. Die Diagnoseprotokolle werden zur Behebung kritischer Probleme wie Systemabstürze in McAfee Advanced Threat Defense benötigt.

Die Inhalte dieser System- oder Diagnoseprotokolldateien können nicht gelesen werden. Diese Protokolle sind für den McAfee-Support gedacht.

Vorgehensweise

1 Klicken Sie auf der Seite **Fehlerbehebung** auf **Protokolldateien**, um die Systemprotokolle herunterzuladen, und auf **Diagnostic File** (Diagnosedatei), um die Diagnoseprotokolle herunterzuladen.

2 Zum Download der sonstigen Informationen und Protokolle klicken Sie auf **Supportpaket**, geben Sie die Ticketnummer ein, und klicken Sie auf **OK**.

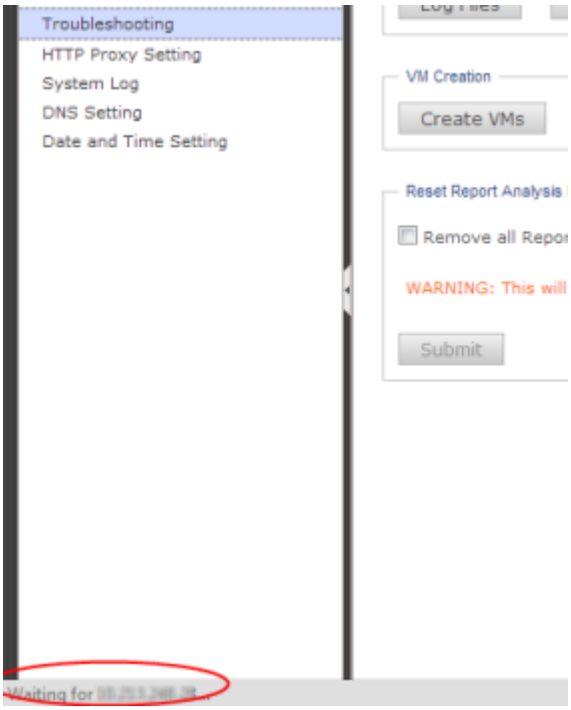


Abbildung 4-8 Erstellung eines Supportpakets

McAfee Advanced Threat Defense sammelt die erforderlichen Informationen. Unten im Browser wird eine Meldung angezeigt. Später wird eine Option zum Speichern der <ticket number>.tgz-Datei angezeigt.

3 Stellen Sie dem McAfee-Support folgende Dateien zur Verfügung:

- Systemprotokolle (atdlogs.bin)
- Diagnoseprotokolle (atdcore.bin)
- Sonstige Protokolltypen (<ticket number>.tgz)

Neuerstellen der Analyse-VMs

Während der dynamischen Analyse können Proben einige der Analyse-VMs beschädigen. Diese Analyse-VM-Instanzen sind daher eventuell nicht für weitere Analysen verfügbar. Unter diesen Umständen können Sie alle bestehenden Analyse-VMs löschen und neu erstellen.

Alle bestehenden Analyse-VMs, einschließlich der Standard-Android-VM und der fehlerfreien Analyse-VMs, werden gelöscht und neu erstellt. Es ist also keine Dateianalyse möglich, bis alle Analyse-VMs erneut erstellt werden. Die Zeit für die Neuerstellung variiert je nach Anzahl der Analyse-VM-Instanzen und deren Größe.

Vorgehensweise

1 Klicken Sie auf der Seite **Troubleshooting** (Fehlerbehebung) auf **Create VMs** (VMs erstellen) und bestätigen Sie, dass Sie alle bestehenden Analyse-VM-Instanzen löschen und neu erstellen möchten.

2 Wählen Sie **Verwalten** | **Systemprotokoll** , um die Protokolle in Zusammenhang mit der Neuerstellung der VMs anzuzeigen.

Sie können **Dashboard** auswählen und den Monitor **VM Creation Status** (VM-Erstellungsstatus) anzeigen, um den Fortschritt der VM-Neuerstellung zu sehen. Die Schaltfläche **Create VMs** (VMs erstellen) auf der Seite **Troubleshooting** (Fehlerbehebung) ist erst wieder verfügbar, nachdem die Analyse-VM-Instanzen neu erstellt wurden.

Löschen der Analyseergebnisse

Vorgehensweise

1 Klicken Sie auf der Seite **Fehlerbehebung** auf **Remove all Report Analysis Results** (Alle Berichtanalyseergebnisse entfernen).

2 Klicken Sie auf **Senden**.

Sichern und Wiederherstellen der Advanced Threat Defense-Datenbank

Als Vorsichtsmaßnahme können Sie die Advanced Threat Defense-Datenbank regelmäßig sichern. Bei Bedarf kann dann die gewünschte Datensicherung wiederhergestellt werden. Wenn Sie beispielsweise alle während einer Fehlerbehebungsübung vorgenommenen Änderungen verwerfen möchten, können Sie die Datensicherung wiederherstellen, die vor Beginn der Fehlerbehebung erstellt wurde.

Sie können täglich, wöchentlich oder monatlich automatische Sicherungen auf einem ausgewählten FTP-Server planen.

Wenn Sie eine Datensicherung wiederherstellen möchten, ruft McAfee Advanced Threat Defense die ausgewählte Sicherungsdatei vom FTP-Server ab und überschreibt die Datenbank mit dem Inhalt der Sicherungsdatei.

Was wird gesichert?

Folgende Daten werden gesichert:

- Die auf der Seite **Analysis Results** (Analyseergebnisse) angezeigten Ergebnisse

  Analyseberichte wie die Analyseübersicht, die gesamten Ergebnisse und Disassembly-Ergebnisse werden nicht gesichert. Wenn die Berichte aus der Datenbank (von der Seite **Troubleshooting** (Fehlerbehebung)) gelöscht werden und dann eine Datensicherung wiederhergestellt wird, werden die auf der Seite **Analysis Results** (Analyseergebnisse) der Datensicherung aufgeführten Ergebnisdetails wiederhergestellt. Die Berichte sind dann jedoch nicht mehr verfügbar.

- Lokale Blacklist (lokale Whitelist wird nicht gesichert)
- VM-Profile

  Die Image- oder VMDK-Datei der Analyse-VMs wird nicht gesichert. Vergewissern sie sich, dass die in den gesicherten VM-Profilen angegebenen Image-Dateien in McAfee Advanced Threat Defense vorhanden sind, bevor Sie eine Datensicherung wiederherstellen.

- Analyseprofile
- Benutzerdatensätze
- Integrationsinformationen zu McAfee ePO
- Proxy-Einstellungen
- DNS-Einstellungen
- Datums- und Uhrzeiteinstellungen einschließlich NTP-Server-Details
- Einstellungen für Lastenausgleichscluster, wie auf der Seite **Load Balancing Cluster Setting** (Einstellungen für Lastenausgleichscluster) dargestellt

  Dies umfasst nicht die Konfigurations- und Analyseergebnisse der anderen Knoten im Cluster.

- Benutzerdefinierte YARA-Regeln und -Konfiguration
- Zeitplaneinstellungen zur Datensicherung
- Gesicherte Dateiinformationen, wie auf der Seite **Restore Management** (Wiederherstellungsverwaltung) dargestellt

Folgende Daten werden nicht gesichert:

- Alle Probedateien oder URLs, die zum Zeitpunkt der Sicherung analysiert werden

  Die Seite **Analysis Status** (Analysestatus) zeigt nur die derzeit analysierte Datei an.

- VMDK- bzw. Image-Dateien von Analyse-VMs
- McAfee Advanced Threat Defense-Software auf der aktiven bzw. der Sicherungsfestplatte
- Protokoll- und Diagnosedateien

Planen einer Datenbanksicherung

Sie können täglich, wöchentlich oder monatlich automatische Sicherungen planen. Der Prozess zur Erstellung der Sicherungen dauert normalerweise einige Minuten. Er variiert je nach Größe der involvierten Daten. McAfee empfiehlt, dass Sie eine Zeit wählen, in der der Umfang der Analysen auf der Advanced Threat Defense wahrscheinlich geringer ist.

Bevor Sie beginnen

- Sie müssen der Administratorbenutzer in der McAfee Advanced Threat Defense-Web-Anwendung sein.
- Sie müssen über einen konfigurierten FTP-Server zum Speichern der Sicherungen verfügen und wissen, in welchem Verzeichnis die Sicherungen gespeichert werden sollen.

- Sie müssen über die IPv4-Adresse des FTP-Servers, den Benutzernamen und das Kennwort für Advanced Threat Defense verfügen, um auf diesen FTP-Server zuzugreifen. Der Benutzername muss außerdem Schreibzugriff auf das Verzeichnis haben, das Sie verwenden möchten.
- Zwischen McAfee Advanced Threat Defense und dem FTP-Server muss die Kommunikation über SFTP oder FTP möglich sein.

Da die Sicherungsfunktion nur für den Administratorbenutzer konfigurierbar ist, sind die FTP-Server-Einstellungen auf der Seite **Backup Scheduler Setting** (Zeitplaneinstellung zur Datensicherung) und die Einstellungen für **FTP Result Output** (FTP-Ergebnisausgabe) auf der Seite **Benutzerverwaltung** für den Administratorbenutzer identisch. Wenn der Administratorbenutzer die FTP-Details auf einer dieser Seiten ändert, spiegelt sich dies daher automatisch auf der anderen Seite wider.

Vorgehensweise

1 Wählen Sie **Verwalten** | **Sichern und wiederherstellen** | **Sichern.**

Die Seite **Backup Scheduler Setting** (Zeitplaneinstellung zur Datensicherung) wird angezeigt.

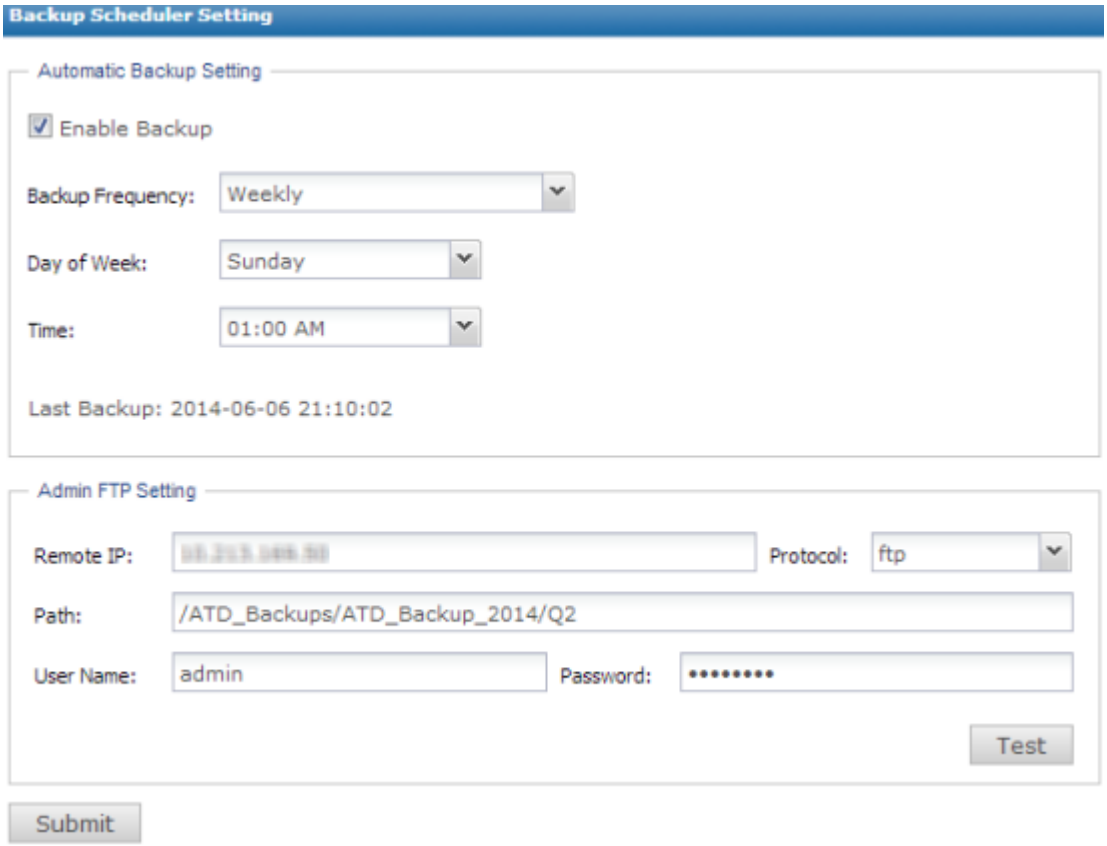


Abbildung 4-9 Planen einer Sicherung

2 Geben Sie die entsprechenden Informationen in die jeweiligen Felder ein.

Optionsname	Beschreibung
Enable Backup (Sicherung aktivieren)	Wählen Sie diese Option, um die automatische Sicherung zur geplanten Zeit zu aktivieren. Wenn Sie die keine automatische Sicherung wünschen, deaktivieren Sie dieses Kontrollkästchen.
Sicherungsintervall	Geben Sie an, wie häufig Advanced Threat Defense eine Sicherung der Datenbank erstellen soll. • **Daily** (Täglich) – Wählen Sie diese Option für eine tägliche Sicherung. **Time** (Uhrzeit) – Geben Sie die Uhrzeit für die tägliche Sicherung an. Wenn Sie z. B. 1:00 Uhr auswählen, führt Advanced Threat Defense die Sicherung täglich um 1:00 Uhr gemäß der integrierten Uhr durch. Für eine sofortige Sicherung können Sie den Befehl `show` auf der Advanced Threat Defense-CLI verwenden, um die aktuelle Zeit auf der Advanced Threat Defense zu erfahren. Mit dem Sicherungsintervall**Daily** (Täglich) können Sie entsprechend eine Uhrzeit für eine sofortige Sicherung angeben. • **Weekly** (Wöchentlich) – Wählen Sie diese Option für eine einmal pro Woche erstellte Sicherung. • **Day of the week** (Wochentag) – Wählen Sie den Tag aus, an dem die Sicherung erstellt werden soll. • **Time** (Uhrzeit) – Geben Sie die Uhrzeit für die Sicherung an dem ausgewählten Tag an. • **Monthly** (Monatlich) – Wählen Sie diese Option für eine einmal pro Monat erstellte Sicherung. • **Day of Month** (Tag des Monats) – Wählen Sie den Tag aus, an dem die Sicherung erstellt werden soll. Wenn Sie z. B. 5 auswählen, erstellt Advanced Threat Defense am fünften jedes Monats eine Sicherung der Datenbank. Sie können nur ein Datum bis 28 angeben. Dadurch werden ungültige Daten, wie 30. Februar, vermieden. • **Time** (Uhrzeit) – Geben Sie die Uhrzeit für die Sicherung an dem ausgewählten Datum an.
Letzte Sicherung	Zeitstempel der letzten erfolgreichen Sicherung.
Remote IP (Remote-IP)	Die IPv4-Adresse des FTP-Servers.
Protokoll	Wählen Sie aus, ob Advanced Threat Defense FTP oder SFTP zur Übertragung der Sicherungsdatei auf den FTP-Server verwenden soll.
Pfad	Das Verzeichnis, in dem Advanced Threat Defense die Datei auf dem FTP-Server speichern muss. Um beispielsweise die Datei im Stammverzeichnis zu speichern, geben Sie Folgendes ein:/.
Benutzername	Der Benutzername, den Advanced Threat Defense verwenden soll, um auf den FTP-Server zuzugreifen. Stellen Sie sicher, dass dieser Benutzername Schreibzugriff auf den angegebenen Ordner hat.
Kennwort	Das entsprechende Kennwort.
Testen	Klicken Sie auf diese Option, um sicherzustellen, dass Advanced Threat Defense mithilfe des ausgewählten Protokolls und der Benutzeranmeldedaten auf den angegebenen FTP-Server zugreifen kann. Sie können eine Sicherung nur erfolgreich planen, wenn die Testverbindung funktioniert.
Senden	Klicken Sie auf diese Option, um die Sicherung zu planen.

3 Zur Anzeige der Protokolle in Zusammenhang mit der Sicherung wählen Sie **Verwalten** | **Systemprotokoll** aus. So können Details wie der Zeitstempel mit Startzeit und Endzeit angezeigt werden.

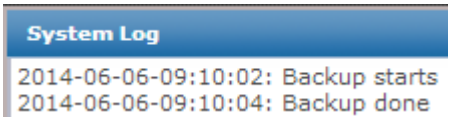


Abbildung 4-10 Protokolle in Zusammenhang mit der Sicherung

Die Sicherung wird in einer kennwortgeschützten ZIP-Datei im angegebenen Verzeichnis auf dem FTP-Server gespeichert.

Versuchen Sie nicht, die Datei zu entpacken oder zu manipulieren. Wenn die Datei beschädigt wird, können Sie die Datenbanksicherung möglicherweise nicht mit dieser Datei wiederherstellen.

Wiederherstellen einer Datenbanksicherung – Spezifische Sicherungsdatei und vorhergehende Sicherungsdatei

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie die FTP-IP-Adresse, den Verzeichnispfad und die Anmeldeinformationen auf der Seite **Backup Scheduler Setting** (Zeitplaneinstellung zur Datensicherung) konfiguriert haben, und prüfen Sie, ob die Verbindung für die angegebene Konfiguration funktioniert. Sie können eine Sicherung nur von dem FTP-Server wiederherstellen, den Sie auch zur Erstellung der Sicherung verwendet haben.
- Vergewissern Sie sich, dass die entsprechende Sicherungsdatei, die Sie wiederherstellen möchten, auf dem FTP-Server im angegebenen Verzeichnis verfügbar ist.
- Vorsichtshalber sollte kein anderer Benutzer während der Wiederherstellung bei Advanced Threat Defense angemeldet sein. Berücksichtigen Sie die Advanced Threat Defense-Web-Anwendung, REST-APIs und CLI.
- Achten Sie darauf, dass Advanced Threat Defense während der Wiederherstellung keine Probedateien oder URLs analysiert. Außerdem dürfen keine integrierten Produkte, Benutzer oder Skripte während der Wiederherstellung Proben einsenden.
- Vergewissern Sie sich, dass Sie während der Sicherung keine Sicherung wiederherstellen.
- Während der Wiederherstellung darf kein Advanced Threat Defense-Software-Upgrade durchgeführt werden.

Mit **Specific backup file** (Spezifische Sicherungsdatei) können Sie die Sicherungsdatei auf dem FTP-Server in jeder Advanced Threat Defense Appliance wiederherstellen. Dies ist hilfreich, wenn die Advanced Threat Defense Appliance beschädigt wird.

Sie können keine Sicherung einer älteren oder neueren Version der Advanced Threat Defense-Software wiederherstellen. Alle Zahlen in der Version müssen genau übereinstimmen. Sie können beispielsweise keine Sicherung von 3.0.4.94.39030 auf 3.0.4.94.39031 wiederherstellen.

Vorgehensweise

1 Wählen Sie **Verwalten** | **Sichern und wiederherstellen** | **Wiederherstellen** aus.

Die Seite **Restore Management** (Wiederherstellungsverwaltung) wird angezeigt.

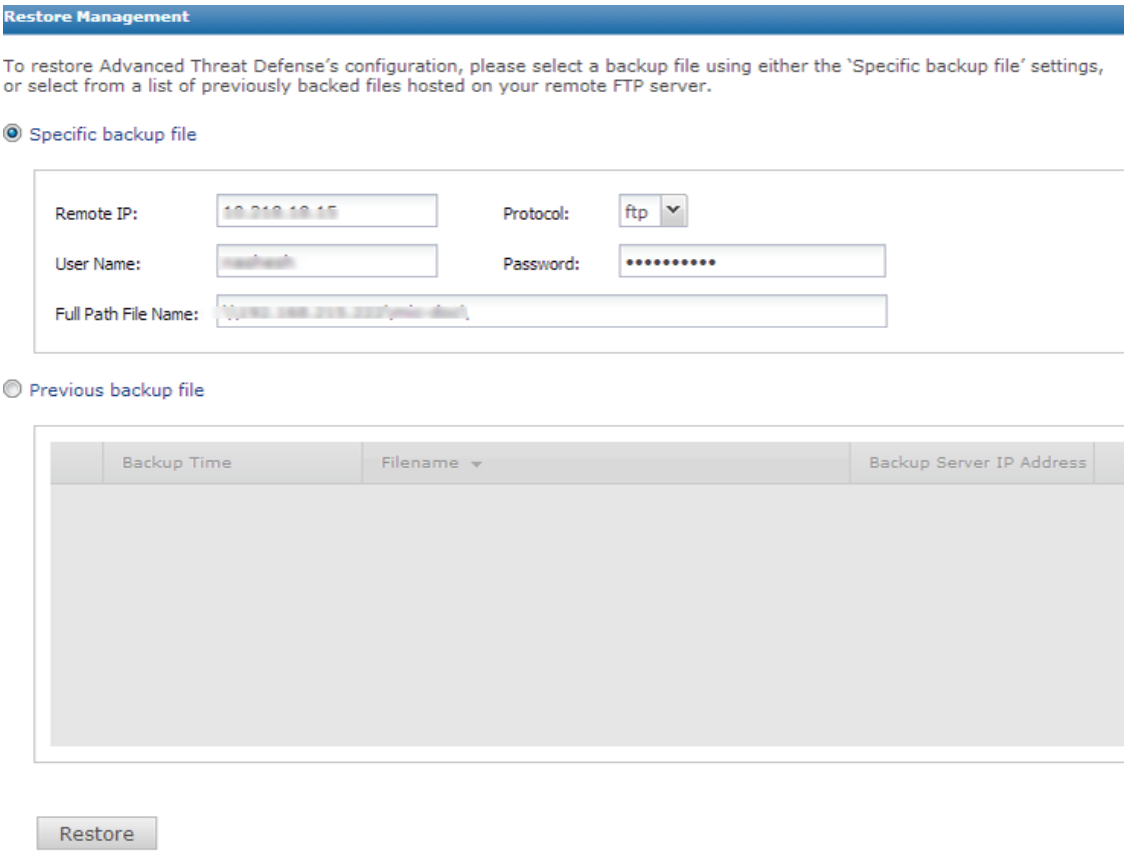

Restore Management
To restore Advanced Threat Defense's configuration, please select a backup file using either the 'Specific backup file' settings, or select from a list of previously backed files hosted on your remote FTP server.
Specific backup file
Remote IP:
Protocol:
ftp
User Name:
Password:
Full Path File Name:
Previous backup file
Backup Time
Filename
Backup Server IP Address
Restore

Abbildung 4-11 Spezifische Sicherungsdatei

2 Wählen Sie **Specific backup file** (Spezifische Sicherungsdatei) aus. Geben Sie die entsprechenden Informationen in die jeweiligen Felder ein.

Tabelle 4-1 Wiederherstellen einer spezifischen Sicherungsdatei

Optionsname	Beschreibung
Remote IP (Remote-IP)	Die IPv4-Adresse des FTP-Servers.
Protokoll	Wählen Sie aus, ob Advanced Threat Defense FTP oder SFTP zur Übertragung der Sicherungsdatei auf den FTP-Server verwenden soll.
Benutzername	Der Benutzername, den Advanced Threat Defense verwenden soll, um auf den FTP-Server zuzugreifen. Stellen Sie sicher, dass dieser Benutzername Schreibzugriff auf den angegebenen Ordner hat.
Kennwort	Das entsprechende Kennwort.
Full Path File Name (Dateiname mit vollständigem Pfad)	Der vollständige Speicherort der zuvor erstellten Datei sowie der Dateiname müssen angegeben werden, damit die Sicherung wiederhergestellt werden kann. Die Wiederherstellung schlägt fehl, wenn die Sicherungsdatei nicht am angegebenen Speicherort auf dem Backup-Server verfügbar ist.

3 Klicken Sie auf **Wiederherstellen**.

Wiederherstellen einer Datenbanksicherung – Vorhergehende Sicherungsdatei

Before you begin

Es kann zu Änderungen bezüglich des für die Sicherung verwendeten FTP-Servers kommen. Beispielsweise kann sich die IP-Adresse des FTP-Backup-Servers ändern, oder Sie möchten den FTP-Server in einen neuen physischen oder virtuellen Server migrieren. Wenn sich die IP-Adresse ändert, stellen Sie sicher, dass Sie die Konfiguration auf der Seite **Backup Scheduler Setting** (Zeitplaneinstellung zur Datensicherung) entsprechend ändern. Sie können anschließend die Wiederherstellung der erforderlichen Sicherungsdatei durchführen. Wurde jedoch der Server selbst geändert, können Sie die Sicherungen auf dem alten Server nicht wiederherstellen. Sie können nur aus den Dateien, die auf dem neuen Server gesichert wurden, wiederherstellen.

- Sie können eine Sicherung nur auf der Advanced Threat Defense Appliance wiederherstellen, aus der die Datenbank gesichert wurde. Sie können beispielsweise keine Sicherung einer Test-Advanced Threat Defense Appliance auf einer Produktions-Advanced Threat Defense Appliance wiederherstellen.
- Sie können keine Sicherung einer älteren oder neueren Version der Advanced Threat Defense-Software wiederherstellen. Alle Zahlen in der Version müssen genau übereinstimmen. Sie können beispielsweise keine Sicherung von 3.0.4.94.39030 auf 3.0.4.94.39031 wiederherstellen.
- Der Prozess zur Wiederherstellung der Sicherungen dauert normalerweise einige Minuten. Er variiert je nach Größe der involvierten Daten.

Task

1 Wählen Sie **Verwalten** | **Sichern und wiederherstellen** | **Wiederherstellen** aus.

Die Seite **Restore Management** (Wiederherstellungsverwaltung) wird angezeigt.

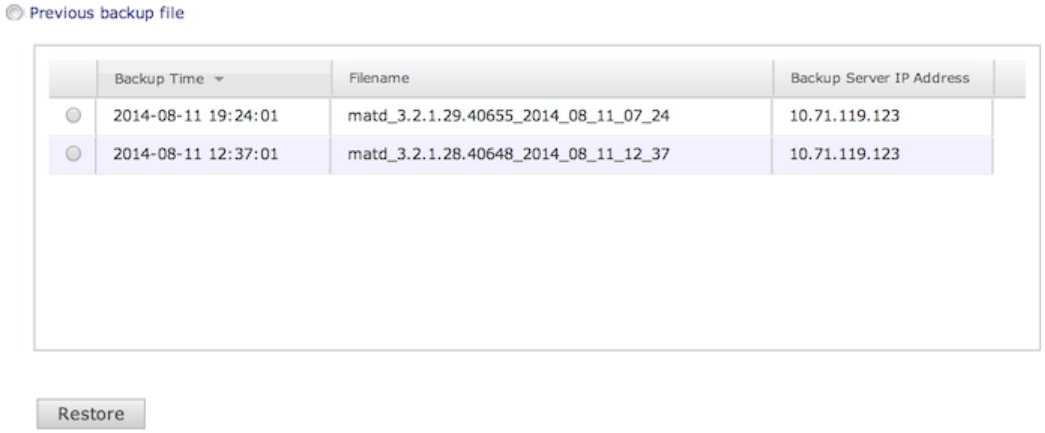


Figure 4-12 Liste der verfügbaren Sicherungsdateien

Table 4-2 Wiederherstellen vorheriger Sicherungsdateien

Optionsname	Beschreibung
File Name (Dateiname)	Der Name, den Advanced Threat Defense der Sicherungsdatei zugewiesen hat. Versuchen Sie nicht, den Dateinamen auf dem FTP-Server zu ändern.
Backup Server IP Address (IP-Adresse des Backup-Servers)	Die IP-Adresse des FTP-Servers, auf dem die Sicherungsdateien gespeichert werden.
Backup Time (Sicherungszeit)	Zeitstempel für die Erstellung der Sicherung.
Wiederherstellen	Wählen Sie die erforderliche Sicherungsdatei aus und klicken Sie auf **Wiederherstellen**, um die Daten aus der Sicherungsdatei wiederherzustellen. Wenn Sie mehr als eine Sicherungsdatei haben, können Sie mit den Optionsfeldern die Sicherungsdateien auswählen, die Sie wiederherstellen möchten.

2 Um die Protokolle in Zusammenhang mit der Wiederherstellung anzuzeigen, wählen Sie **Verwalten** | **Systemprotokoll**.

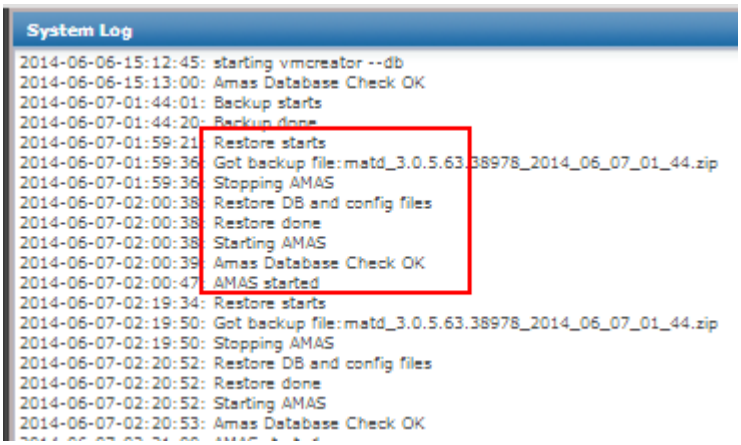


Figure 4-13 Protokolle in Zusammenhang mit der Datenwiederherstellung

Die Prozesse in Zusammenhang mit der Probenanalyse werden vor der Wiederherstellung angehalten und nach der Wiederherstellung neu gestartet.

5

Erstellen einer Analyse-VM

In der dynamischen Analyse führt McAfee Advanced Threat Defense eine verdächtige Datei auf einem sicheren virtuellen Computer (Virtual Machine, VM) aus und überwacht ihr Verhalten hinsichtlich böswilliger Aktivitäten. Diese VM wird als Analyse-VM bezeichnet. In diesem Kapitel werden die Schritte zum Erstellen einer Analyse-VM und des VM-Profils beschrieben.



Jede Sicherheitssoftware bzw. jedes einfache Dienstprogramm auf einer Analyse-VM kann zu Konflikten mit der dynamischen Analyse der Probedatei führen. Die Ausführung der Probedatei selbst kann während der dynamischen Analyse abgebrochen werden. Aufgrund dessen könnten die Berichte nicht das gesamte Verhalten der Probedatei erfassen. Wenn Sie das vollständige Verhalten der Probedatei ermitteln möchten, sollten Sie das Betriebssystem der Analyse-VM mit keinem Patch versehen und keine Sicherheitssoftware darauf installieren. Wenn Sie die Auswirkung der Probedatei speziell auf Ihr Netzwerk ermitteln möchten, verwenden Sie Ihr COE(Common Operating Environment)-Image mit der regulären Sicherheitssoftware, um die Analyse-VMs zu erstellen.

Die Hauptschritte zum Erstellen einer Analyse-VM und des VM-Profils sind wie folgt:

1 Erstellen Sie ein ISO-Image des entsprechenden Betriebssystems. Sie müssen außerdem über den Lizenzschlüssel für das Betriebssystem verfügen. Um beispielsweise eine Analyse-VM für Windows 7 zu erstellen, müssen Sie über ein ISO-Image von Windows 7 und den Lizenzschlüssel verfügen.

   Für das Erstellen der Analyse-VMs werden nur die folgenden Betriebssysteme unterstützt:

   - Microsoft Windows XP (32 Bit), Service Pack 2
   - Microsoft Windows XP (32 Bit), Service Pack 3
   - Microsoft Windows Server 2003 (32 Bit), Service Pack 1
   - Microsoft Windows Server 2003 (32 Bit), Service Pack 2
   - Microsoft Windows Server 2008 R2, Service Pack 1
   - Microsoft Windows 7 (32 Bit), Service Pack 1
   - Microsoft Windows 7 (64 Bit), Service Pack 1
   - Microsoft Windows 8.0 Pro (32 Bit)

- Microsoft Windows 8.0 Pro (64 Bit)
- Standardmäßig Android 2.3. Sie können ein Upgrade auf Android 4.3 durchführen. Siehe Upgrade der Android-Analyse-VM auf Seite 55.

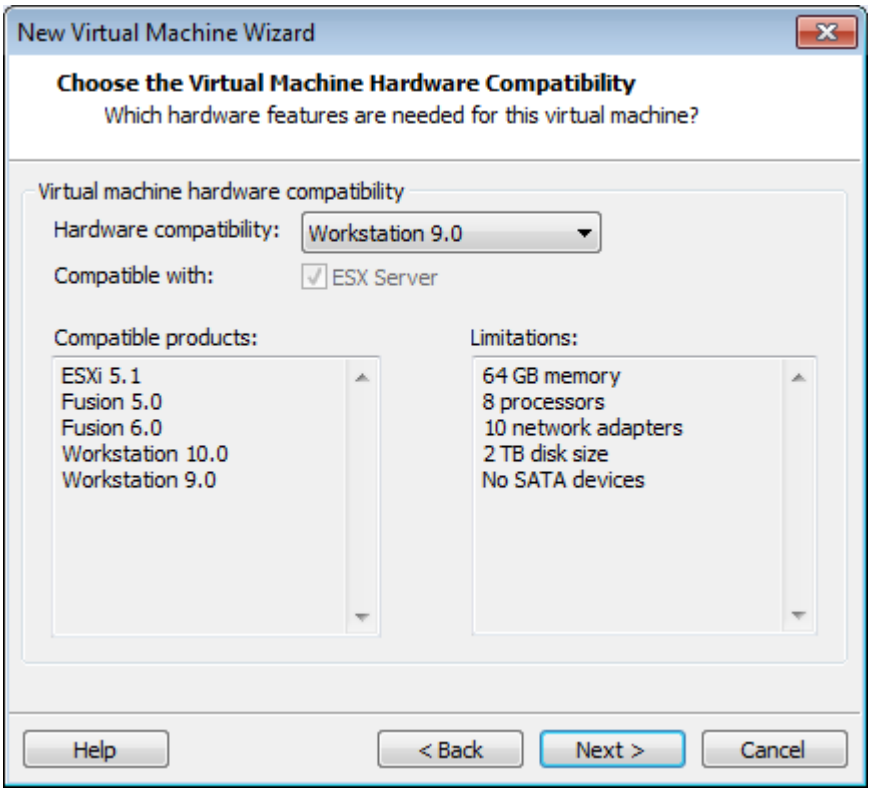
Die oben genannten Windows-Betriebssysteme können auf Deutsch, Englisch, Chinesisch (vereinfacht), Japanisch oder Italienisch vorliegen.

Die einzige vorinstallierte Analyse-VM ist die Android-VM.

2 Beim Verwenden der VMware Workstation 9.0 wird eine VMDK(Virtual Machine Disk)-Datei der ISO-Datei erstellt. Nach dem Erstellen der VM können Sie erforderliche Anwendungen installieren, beispielsweise:

- Internet Explorer 6, 7, 8, 9 und 10
- Firefox 11, 12 und 13
- Microsoft Office 2003, 2007, 2010 oder 2013
- Adobe Reader 8, 9 oder 10

Die empfohlene VMware Workstation-Version ist 9.0. Wenn Sie jedoch VMware Workstation 10.0 verwenden, wählen Sie im Fenster **New Virtual Machine Wizard** (Assistent für neue virtuelle Computer) unter **Hardware Compatibility** (Hardwarekompatibilität) **Workstation 9.0** aus (siehe unten).



3 Importieren Sie die VMDK-Datei in die McAfee Advanced Threat Defense Appliance.

4 Konvertieren Sie die VMDK-Datei in eine Image-Datei (IMG).

5 Erstellen Sie die VM und das VM-Profil.

Wenn bereits eine VMDK-Datei vorhanden ist, muss sie eine einzelne Datei sein, die alle zur VM-Erstellung benötigten Dateien enthält.

In der nachstehenden Tabelle wird die maximale Anzahl von VMs angegeben, die abhängig von der jeweiligen Windows-Version erstellt werden können.

Tabelle 5-1 VM-Anzahl nach Betriebssystem

Windows-Betriebssystem	ATD-3000 (VM-Anzahl)	ATD-6000 (VM-Anzahl)
WinXP SP2 (5 GB)	29	59
WinXP SP3 (5 GB)	29	59
Windows 2003 SP1 (5 GB)	29	59
Windows 2003 SP2 (5 GB)	29	59
Windows 2008 64 Bit SP1 (14 GB)	22	45
Windows 7 32 Bit (14 GB)	22	45
Windows 7 64 Bit (14 GB)	22	45
Windows 8 32 Bit (24 GB)	22	45
Windows 8 64 Bit (24 GB)	22	45

Die Android-VM ist die Standard-VM für alle ATD-Installationen.

Inhalt

- *Erstellen einer VMDK-Datei für Windows XP*
- *Erstellen einer VMDK-Datei für Windows 2003 Server*
- *Erstellen einer VMDK-Datei für Windows 7*
- *Erstellen einer VMDK-Datei für Windows 2008 Server*
- *Erstellen einer VMDK-Datei für Windows 8*
- *Importieren einer VMDK-Datei in McAfee Advanced Threat Defense*
- *Konvertieren der VMDK-Datei in eine Image-Datei*
- *Verwalten von VM-Profilen*
- *Anzeigen des VM-Erstellungsprotokolls*

Erstellen einer VMDK-Datei für Windows XP

Bevor Sie beginnen

- Laden Sie VMware Workstation 9.0 oder höher von der Seite http://www.vmware.com/products/workstation/workstation-evaluation herunter, und installieren Sie das Programm.
- Stellen Sie sicher, dass Sie über ein ISO-Image von Windows XP SP2 oder SP3 verfügen, für das Sie die VMDK-Datei erstellen müssen. Nur Windows Professional wird unterstützt.
- Stellen Sie sicher, dass Sie über den Lizenzschlüssel für das Betriebssystem verfügen.

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3.

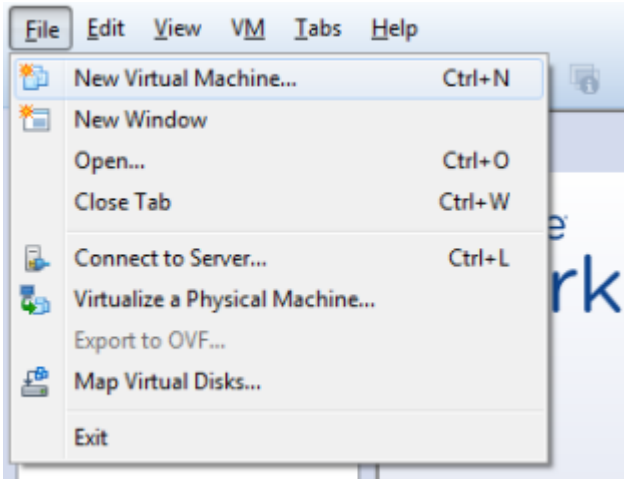
Schritt	Details
Schritt 1: Starten Sie VMware Workstation.	In diesem Beispiel wird VMware Workstation 10 verwendet.
Schritt 2: Wählen Sie auf der VMware Workstation-Seite **File (Datei) | New Virtual Machine (Neuer virtueller Computer).**	
Schritt 3: Wählen Sie im Fenster **New Virtual Machine Wizard** (Assistent für neue virtuelle Computer) die Option **Custom (Advanced)** (Benutzerdefiniert (erweitert)), und klicken Sie auf **Next** (Weiter).	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

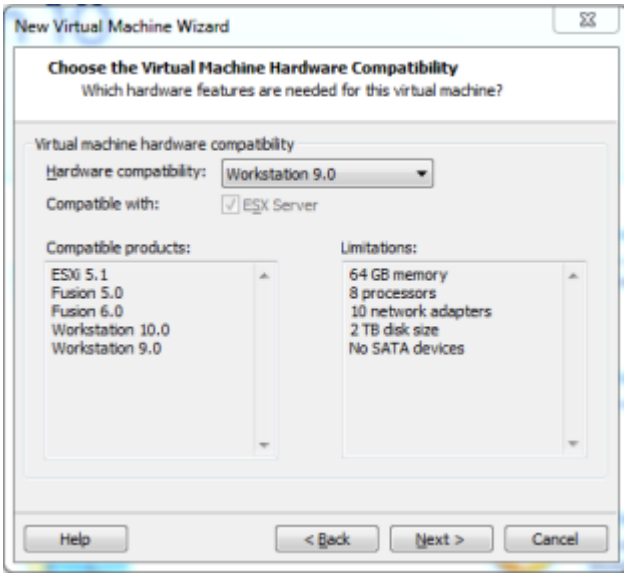
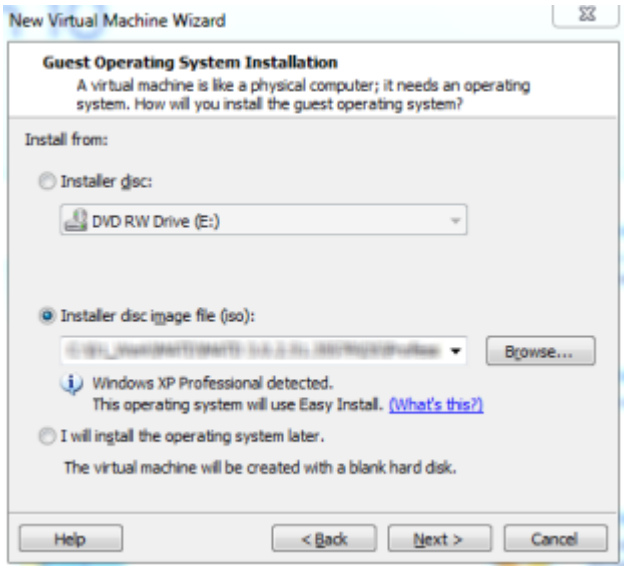
Schritt	Details
Schritt 4: Wählen Sie im Fenster **Choose the Virtual Machine Hardware Compatibility** (Wählen der Hardwarekompatibilität des virtuellen Computers) **Workstation 9.0** aus der Dropdown-Liste **Hardware compatibility** (Hardwarekompatibilität) aus. Akzeptieren Sie bei den anderen Feldern die Standardwerte, und klicken Sie auf **Next** (Weiter).	
Schritt 5: Wählen Sie im Fenster **Guest Operating System Installation** (Installation eines Gast-Betriebssystems) entweder **Installer disc** (Installationsdatenträger) oder **Installer disc image file (iso)** (Image-Datei des Installationsdatenträgers), navigieren Sie zum ISO-Image, wählen Sie es aus, und klicken Sie anschließend auf **Next** (Weiter).	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

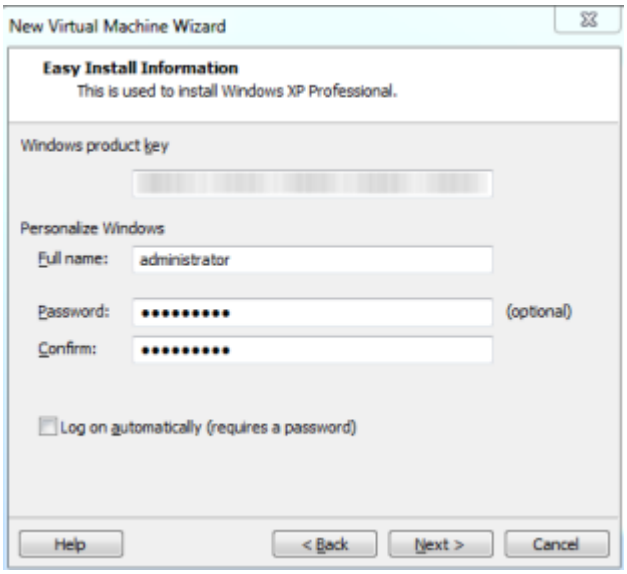
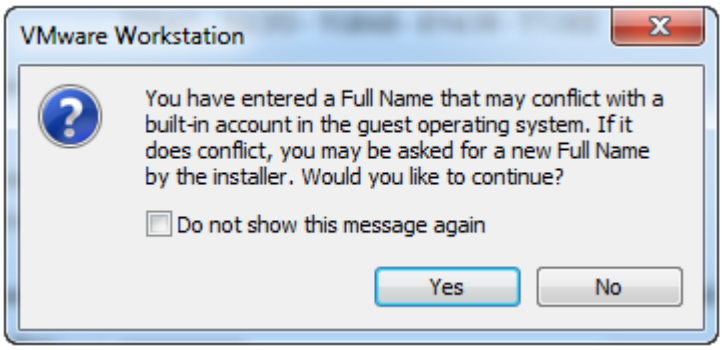
Schritt	Details
Schritt 6: Geben Sie die Informationen im Fenster **Easy Install Information** (Informationen zur einfachen Installation) ein, und klicken Sie auf **Next** (Weiter).	• **Windows product key** (Windows-Produktschlüssel) – Geben Sie den Lizenzschlüssel des Windows-Betriebssystems ein, für das Sie die VMDK-Datei erstellen. • **Full name** (Vollständiger Name) – Geben Sie `administrator` als **Full name** ein. • **Password** (Kennwort) – Geben Sie `cr@cker42` als Kennwort ein. Dies ist das Kennwort, das McAfee Advanced Threat Defense für die Anmeldung bei der VM verwendet. • **Confirm** (Bestätigen) – Geben Sie `cr@cker42` zur Bestätigung erneut ein. • **Log on automatically (requires a password)** (Automatisch anmelden; Kennwort erforderlich) – Deaktivieren Sie dieses Kontrollkästchen. 
Schritt 7: Klicken Sie im Popupfenster **VMware Workstation** auf **Yes** (Ja).	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

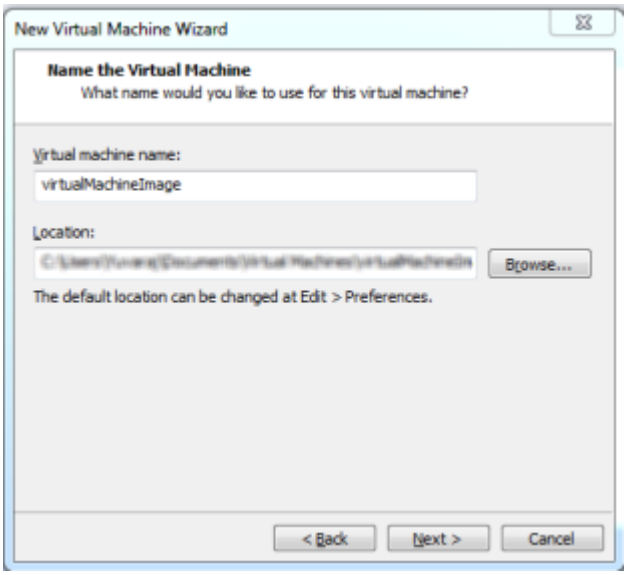
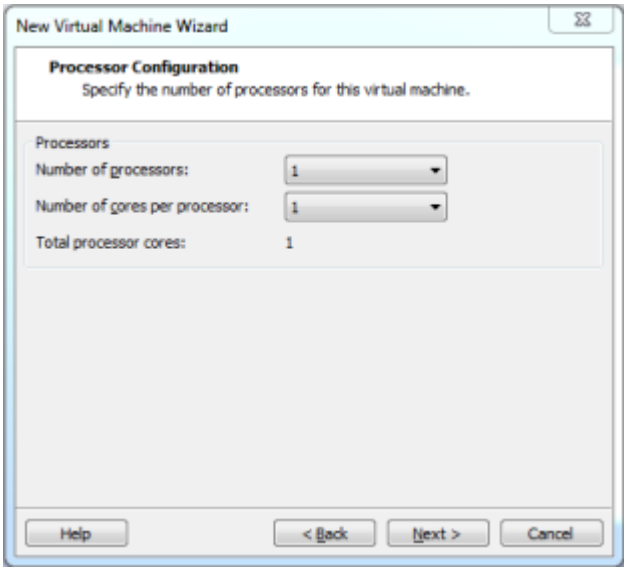
Schritt	Details
Schritt 8: Geben Sie die Informationen im Fenster **Name the Virtual Machine** (Benennen des virtuellen Computers) ein, und klicken Sie anschließend auf **Next** (Weiter).	• **Virtual Machine name** (Name des virtuellen Computers) – Geben Sie `virtualMachineImage` als Namen ein. • **Location** (Speicherort) – Navigieren Sie zu dem Ordner, in dem die VDMK-Datei erstellt werden soll, und wählen Sie ihn aus. 
Schritt 9: Übernehmen Sie im Fenster **Processor Configuration** (Prozessorkonfiguration) die Standardwerte, und klicken Sie auf **Next** (Weiter).	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

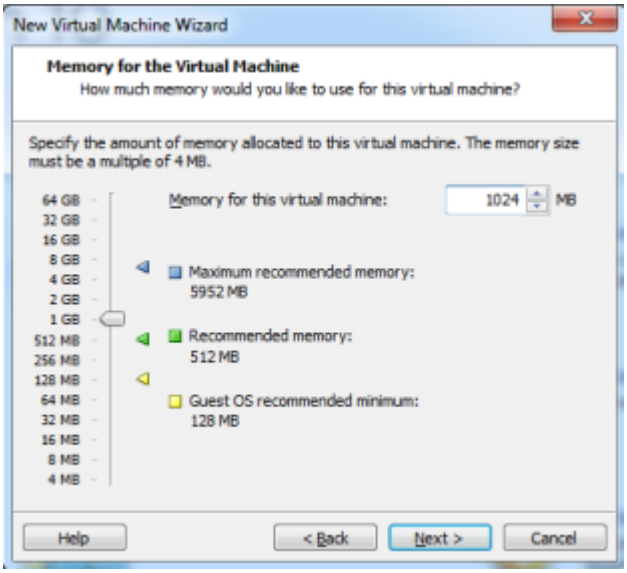
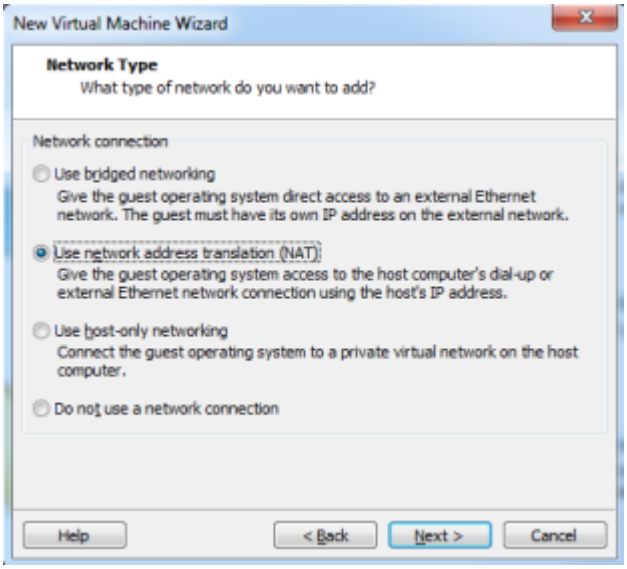
Schritt	Details
Schritt 10: Legen Sie im Fenster **Memory for the Virtual Machine** (Speicher für den virtuellen Computer) 1.024 MB als Speicher fest.	
Schritt 11: Übernehmen Sie im Fenster **Network Type** (Netzwerktyp) die Standardauswahl.	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

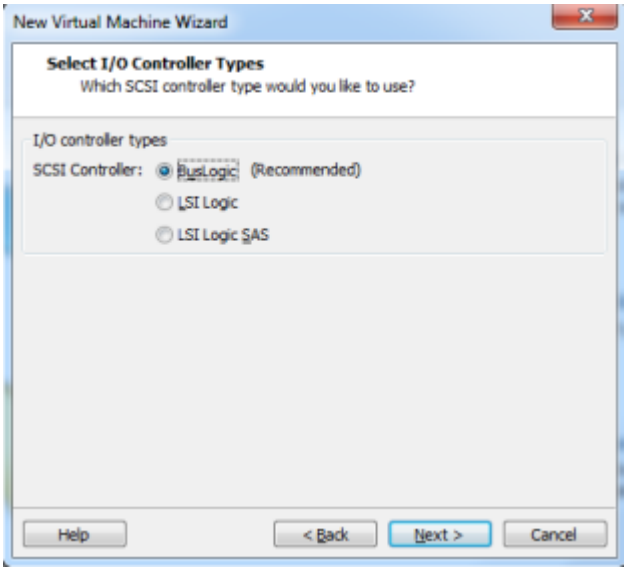
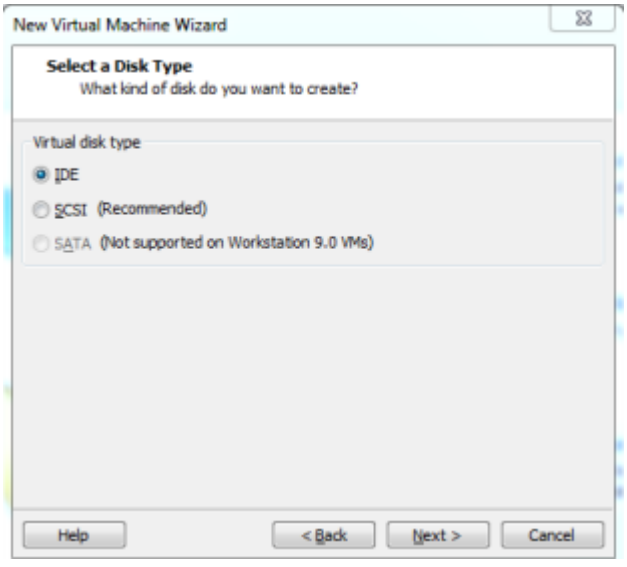
Schritt	Details
Schritt 12: Übernehmen Sie unter **Select I/O Controller Types** (Auswählen der I/O-Controller-Typen) die Standardauswahl.	
Schritt 13: Wählen Sie auf der Seite **Auswählen eines Datenträgertyps** die Option **IDE**, und klicken Sie auf **Next** (Weiter). SCSI-Datenträger sind mit McAfee Advanced Threat Defense nicht kompatibel.	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

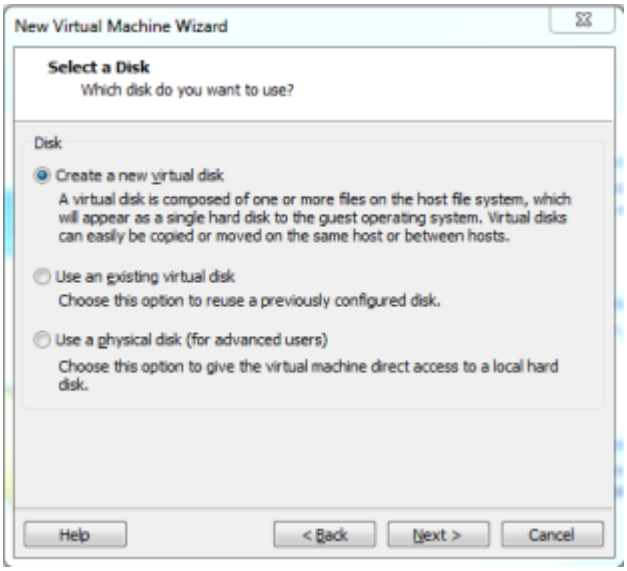
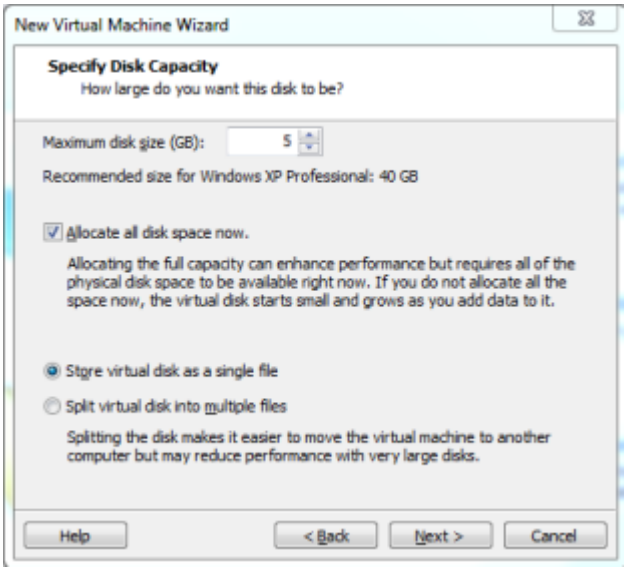
Schritt	Details
Schritt 14: Wählen Sie im Fenster **Auswählen eines Datenträgers** die Option **Create a new virtual disk** (Neuen virtuellen Datenträger erstellen), und klicken Sie auf **Next** (Weiter).	
Schritt 15: Geben Sie die Details im Fenster **Angeben der Speicherkapazität** an, und klicken Sie auf **Next** (Weiter).	• **Maximum disk size (GB)** (Maximale Datenträgergröße (GB)): Für Windows XP beträgt die maximale Datenträgergröße 30 GB. Geben Sie jedoch 5 GB ein, um eine optimale Leistung zu gewährleisten. • Wählen Sie **Allocate all disk space now** (Sämtlichen Speicherplatz jetzt zuweisen). • Wählen Sie **Store virtual disk as a single file** (Virtuellen Datenträger als einzelne Datei speichern). 

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

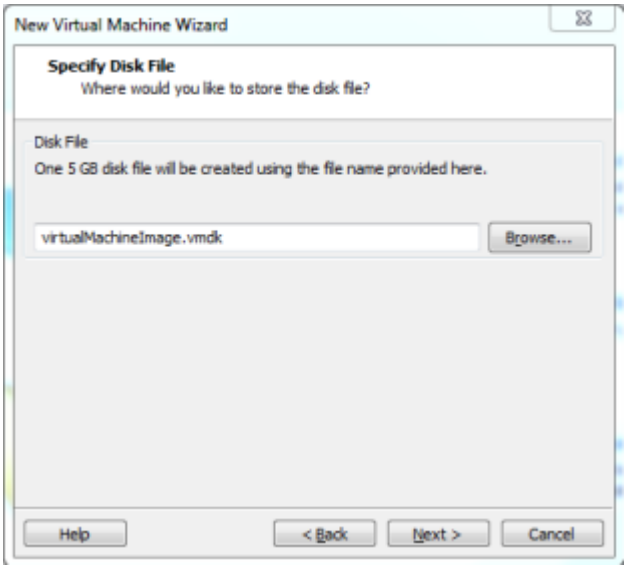
Schritt	Details
Schritt 16: Vergewissern Sie sich, dass im Fenster **Specify Disk file** (Datenträgerdatei angeben) standardmäßig "virtualMachineImage.vmdk" angezeigt wird, und klicken Sie auf **Next** (Weiter). Wenn Sie unter **Virtual Machine name** (Name des virtuellen Computers) einen anderen Namen angegeben haben, wird dieser hier angezeigt.	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

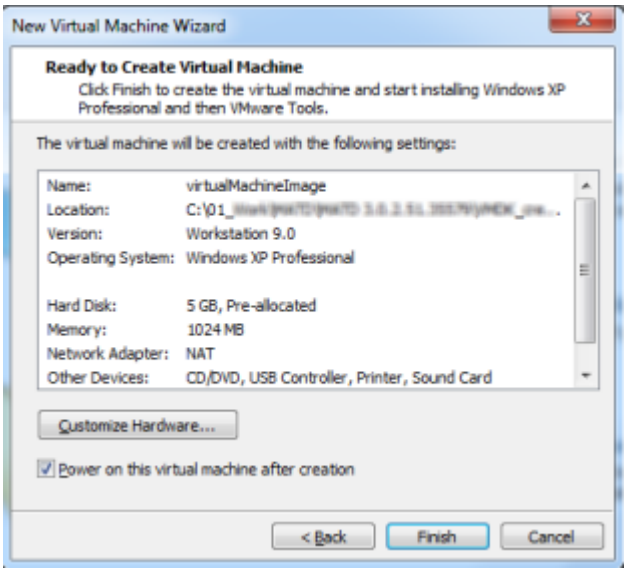
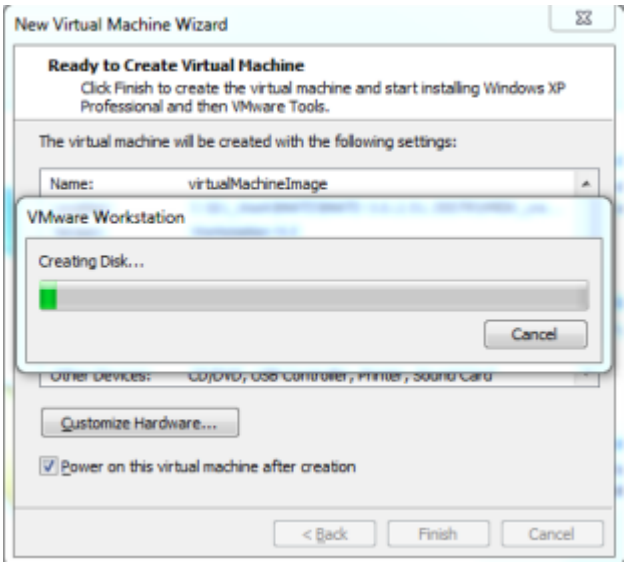
Schritt	Details
Schritt 17: Führen Sie folgende Schritte im Fenster **Ready to Create Virtual Machine** (Bereit zur Erstellung des virtuellen Computers) aus.	• **Power on this virtual machine after creation** (Diesen virtuellen Computer nach der Erstellung einschalten) – Wählen Sie diese Option. • Klicken Sie auf **Finish** (Fertig stellen). Dieser Schritt kann etwa 30 Minuten in Anspruch nehmen.  
Schritt 18: Wenn das Popupfenster **Removable Devices** (Wechselgeräte) angezeigt wird, wählen Sie **Do not show this hint again** (Diesen Hinweis nicht mehr anzeigen), und klicken Sie auf **OK**.	Die Installation von Windows beginnt. Dies kann etwa 15 Minuten dauern.

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

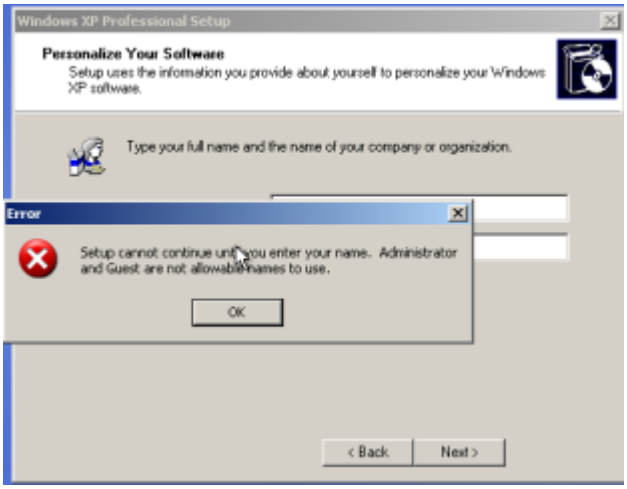
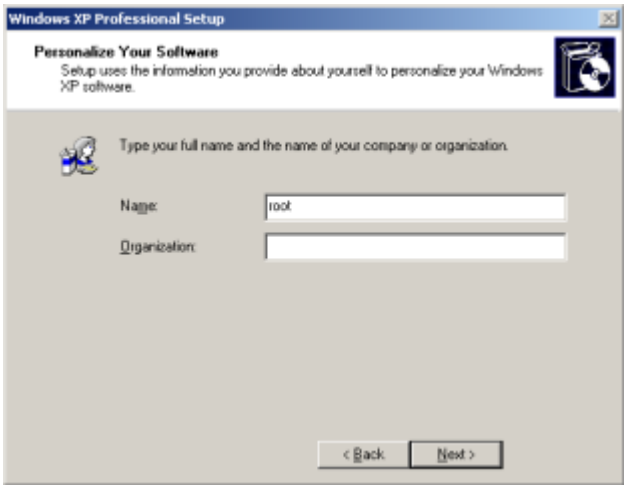
Schritt	Details
Schritt 19: Klicken Sie auf **OK**, wenn die folgende Fehlermeldung angezeigt wird: *Setup kann nicht fortgesetzt werden, solange Sie Ihren Namen nicht eingegeben haben. "Administrator" und "Guest" können nicht verwendet werden.*	
Schritt 20: Geben Sie die folgenden Informationen im Fenster **Windows XP Professional Setup** (Einrichtung für Windows XP Professional) ein.	• **Name:** Geben Sie `root` ein. • **Organisation:** Lassen Sie dieses Feld leer, und klicken Sie auf **Weiter**. Dieser Vorgang kann etwa 15 Minuten in Anspruch nehmen. 
Schritt 21: Nur wenn Sie dazu aufgefordert werden, melden Sie sich mit den folgenden Anmeldeinformationen beim virtualMachineImage an.	• **User** (Benutzer): `administrator` • **Password** (Kennwort): `cr@cker42`

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

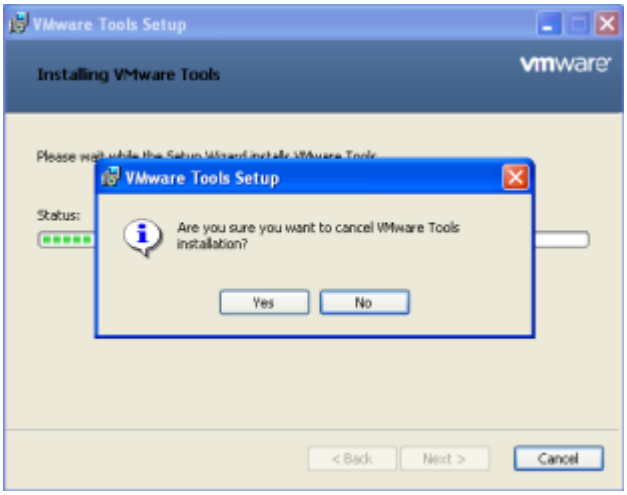
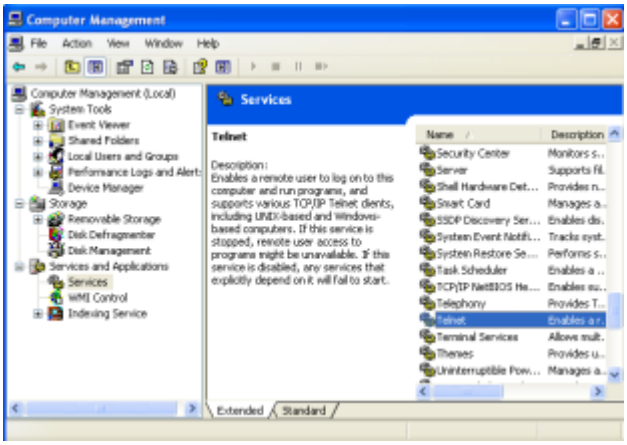
Schritt	Details
Schritt 22: Halten Sie die Installation von VMware Tools an. Die VMware Tools sind mit McAfee Advanced Threat Defense nicht kompatibel. Wenn Sie die Installation von VMware Tools nicht angehalten haben, können Sie dennoch mit der VMDK-Dateierstellung fortfahren. Das Programm muss aber deinstalliert sein, sobald die VMDK-Datei bereit ist.	
Schritt 23: Wählen Sie im virtualMachineImage die Optionen **Start** | **Systemsteuerung** | **Sicherheitscenter** | **Windows-Firewall** | **AUS**.	
Schritt 24: Klicken Sie im virtualMachineImage auf **Start** und dann mit der rechten Maustaste auf **Arbeitsplatz**. Wählen Sie dann **Verwalten** | **Dienste und Anwendungen** | **Dienste**. Doppelklicken Sie anschließend auf **Telnet**.	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

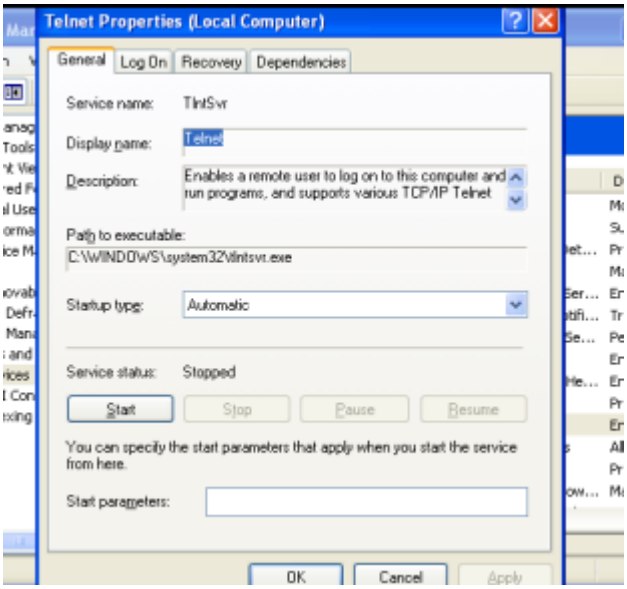
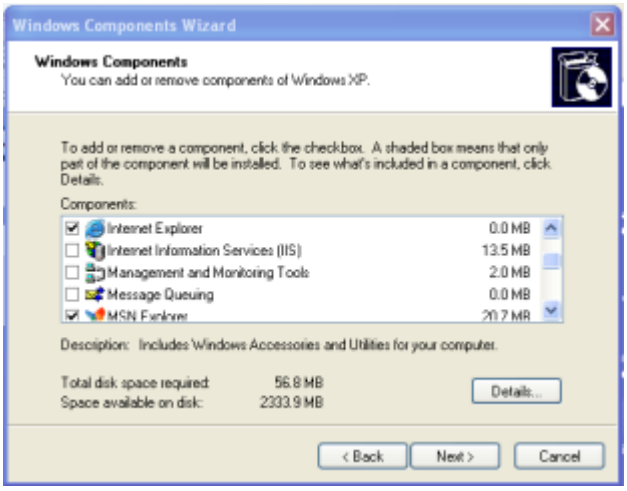
Schritt	Details
Schritt 25: Wählen Sie im Fenster **Eigenschaften von Telnet (Lokaler Computer)** aus der Dropdown-Liste **Starttyp** die Option **Automatisch.** Wählen Sie dann **Anwenden** | **Start** | **OK.**	
Schritt 26: Aktivieren Sie FTP auf der VM. Wählen Sie im virtualMachineImage die Optionen **Start** | **Systemsteuerung** | **Software** | **Windows-Komponenten hinzufügen oder entfernen.**	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

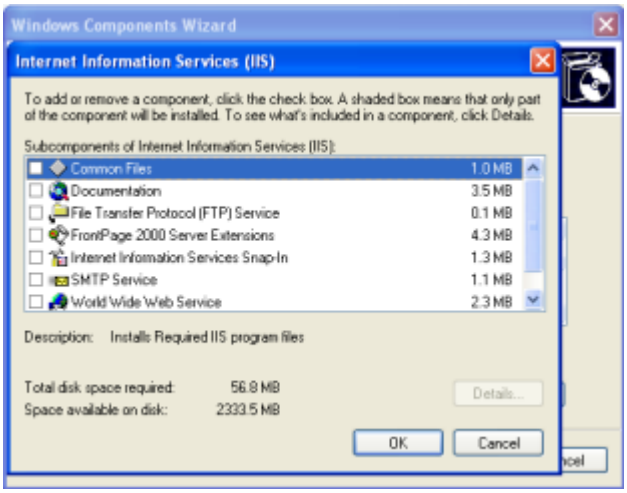
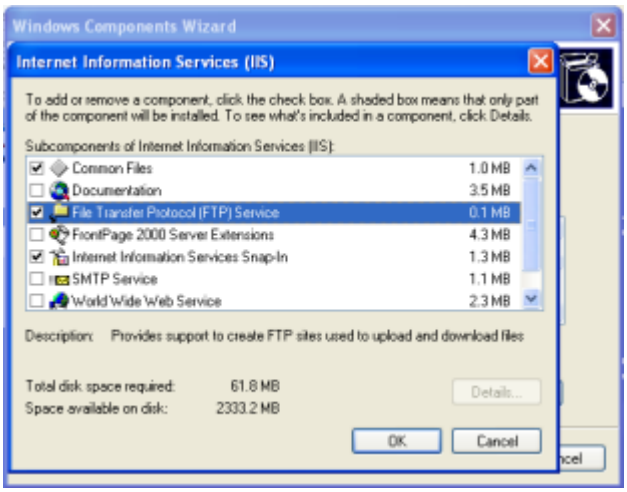
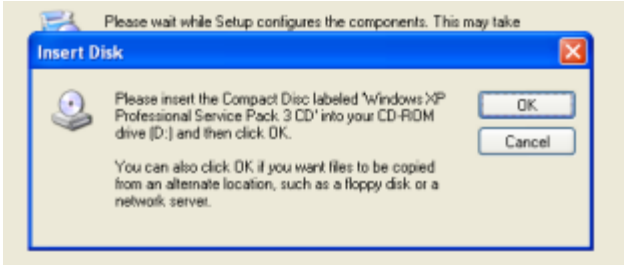
Schritt	Details
Schritt 27: Doppelklicken Sie im **Assistenten für Windows-Komponenten** auf **Internetinformationsdienste (IIS).**	
Schritt 28: Führen Sie im Popupfenster **Internetinformationsdienste (IIS)** die folgenden Schritte aus.	1 Wählen Sie **FTP-Dienst (File Transfer Protocol).** 2 Wählen Sie **Gemeinsame Dateien.** 3 Wählen Sie **Internetinformationsdienste-Snap-In,** klicken Sie auf **OK** und anschließend auf **Weiter.** 
Schritt 29: Klicken Sie im Pop-Up **Datenträger einlegen** auf **Abbrechen.**	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

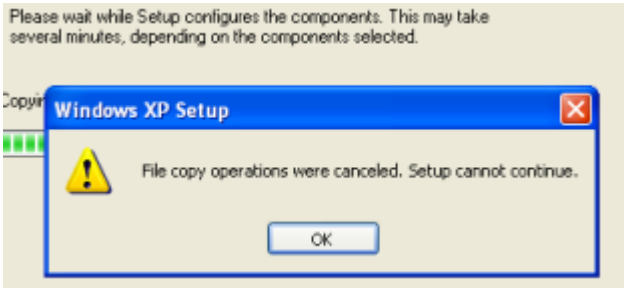
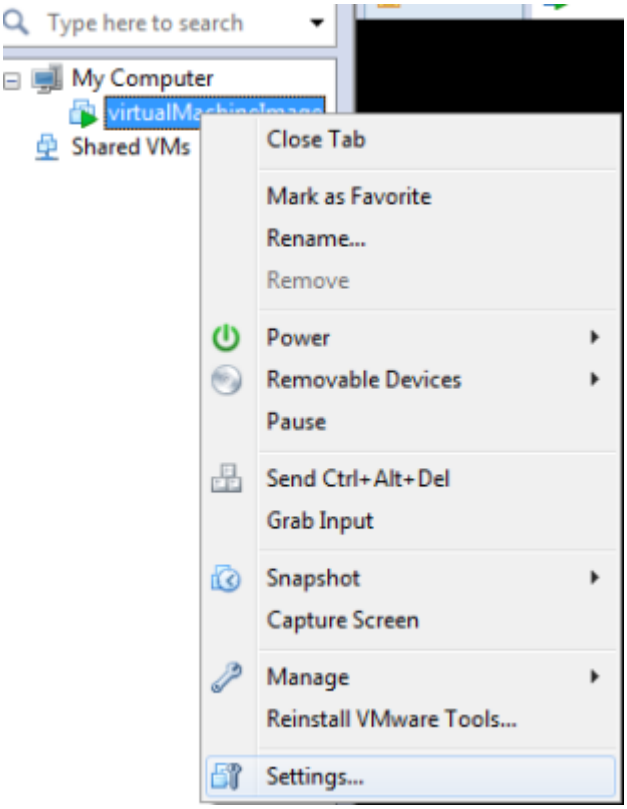
Schritt	Details
Schritt 30: Wählen Sie im Pop-Up **Windows XP Setup** die Option **OK** aus.	
Schritt 31: Klicken Sie in VMware Workstation mit der rechten Maustaste auf die VM, in diesem Beispiel "virtualMachineImage". Wählen Sie dann **Einstellungen** aus.	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

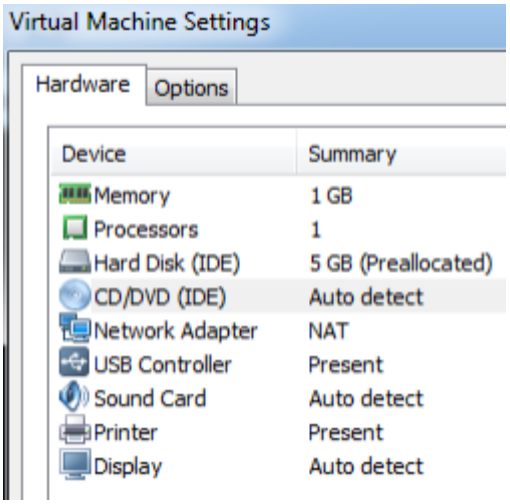
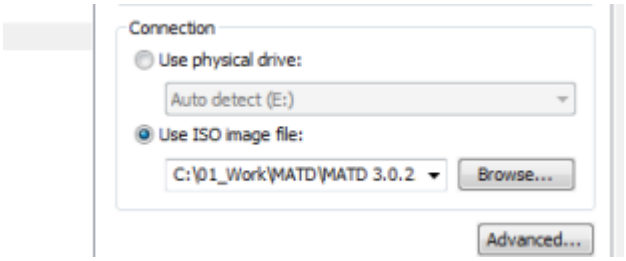
Schritt	Details
Schritt 32: Wählen Sie im Fenster "Einstellungen des virtuellen Computers" den Eintrag **CD/DVD (IDE)** aus.	
Schritt 33: Navigieren Sie im Feld **Use ISO image file** (ISO-Image-Datei verwenden) zum ISO-Image, das Sie verwendet haben, und klicken Sie auf **OK**.	
Schritt 34: Klicken Sie im Fenster **Willkommen bei Microsoft Windows XP** auf **Beenden**.	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

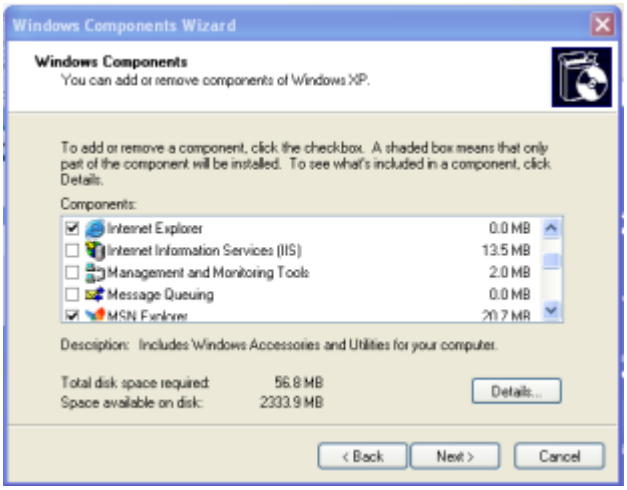
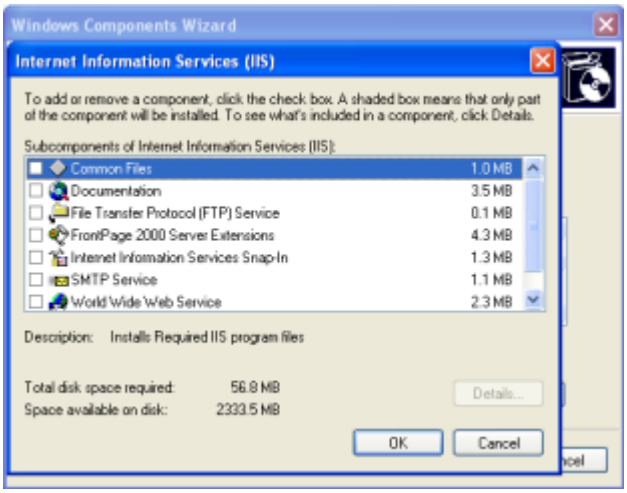
Schritt	Details
Schritt 35: Wählen Sie im virtualMachineImage die Optionen **Start** | **Systemsteuerung** | **Software** | **Windows-Komponenten hinzufügen oder entfernen.**.	
Schritt 36: Doppelklicken Sie im **Assistenten für Windows-Komponenten** auf **Internetinformationsdienste (IIS).**	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

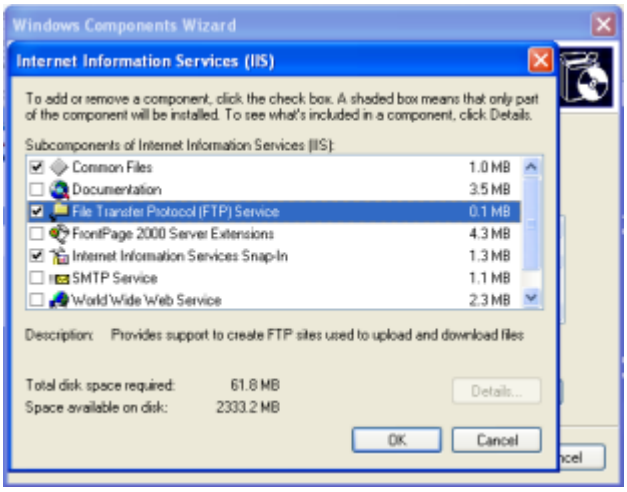
Schritt	Details
Schritt 37: Führen Sie im Popupfenster **Internetinformationsdienste (IIS)** die folgenden Schritte aus.	1 Wählen Sie **FTP-Dienst (File Transfer Protocol)**. 2 Wählen Sie **Gemeinsame Dateien**. 3 Wählen Sie **Internetinformationsdienste-Snap-In**, klicken Sie auf **OK** und anschließend auf **Weiter**. 
Schritt 38: Klicken Sie im **Assistenten für Windows-Komponenten** auf **Beenden**, um die Installation von FTP abzuschließen.	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

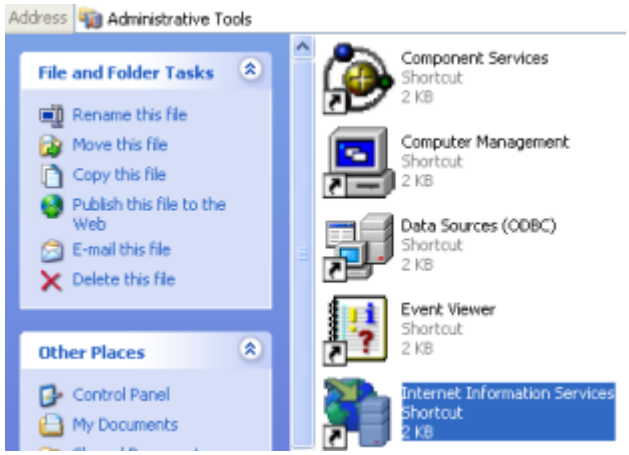
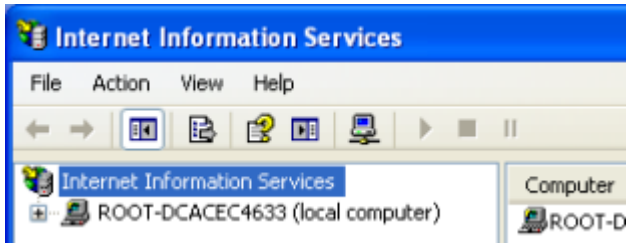
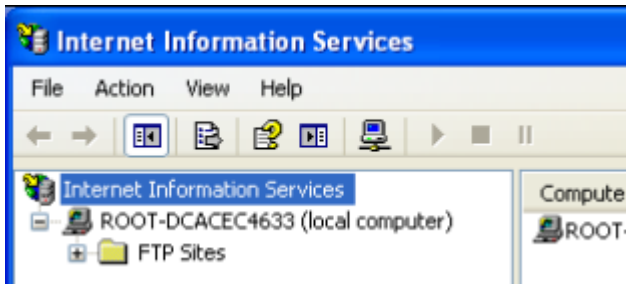
Schritt	Details
Schritt 39: Wählen Sie **Start** | **Systemsteuerung** | **Zur klassischen Ansicht wechseln** | **Verwaltung** , und doppelklicken Sie auf **Internetinformationsdienste**.	
Schritt 40: Erweitern Sie im Fenster **Internetinformationsdienste** den Eintrag **Internetinformationsdienste**.	
Schritt 41: Erweitern Sie das Fenster **FTP-Sites**.	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

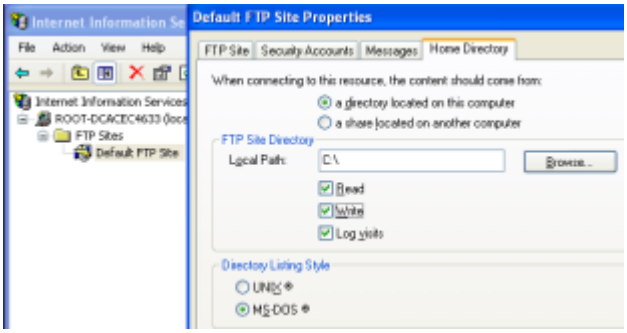
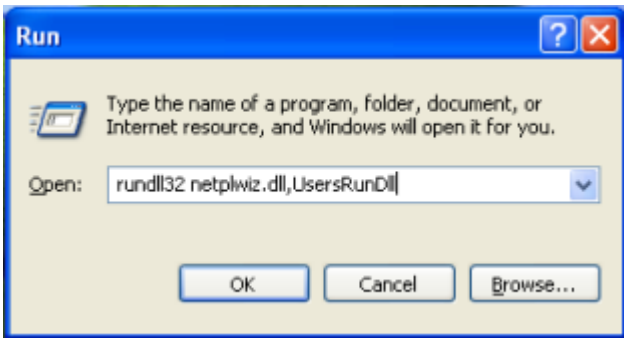
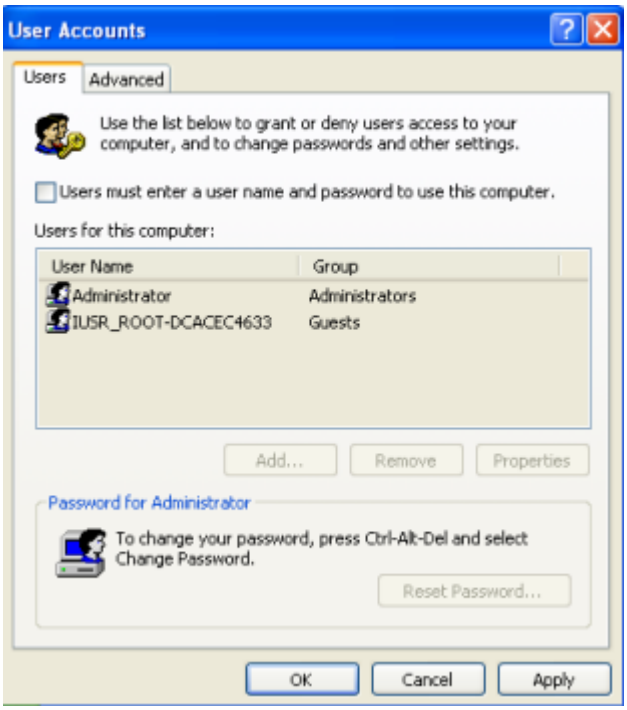
Schritt	Details
Schritt 42: Klicken Sie mit der rechten Maustaste auf **Standard-FTP-Site**, und wählen Sie dann **Eigenschaften** | **Basisverzeichnis**. Führen Sie dann folgende Schritte aus. 1 Navigieren Sie zu C:\ 2 Wählen Sie **Lesen**. 3 Wählen Sie **Schreiben**. 4 Wählen Sie **Besuche protokollieren**, und klicken Sie auf **Übernehmen** und anschließend auf **OK**.	
Schritt 43: Richten Sie die automatische Anmeldung ein, indem Sie **Start** | **Ausführen**auswählen, `rundll32 netplwiz.dll,UsersRunDll` eingeben und die **Eingabetaste** drücken.	
Schritt 44: Deaktivieren Sie im Fenster **Benutzerkonten** die Option **Benutzer müssen Benutzernamen und Kennwort eingeben**, und klicken Sie auf **Übernehmen**.	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

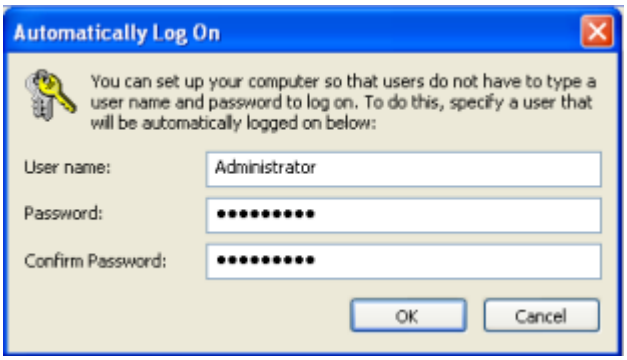
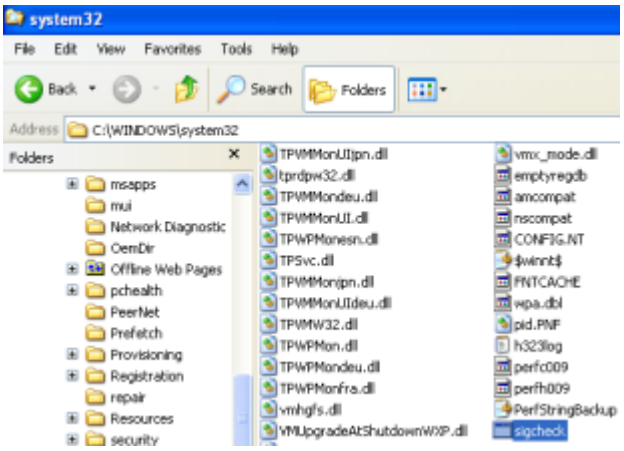
Schritt	Details
Schritt 45: Führen Sie im Popupfenster **Automatische Anmeldung** die folgenden Schritte aus, und klicken Sie dann auf **OK**.	• **Benutzername** – Geben Sie `Administrator` ein. • **Kennwort** – Geben Sie `cr@cker42` ein. • **Kennwort bestätigen** – Geben Sie `cr@cker42` erneut ein. 
Schritt 46: Laden Sie Sigcheck von der Seite http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx auf Ihren Computer (den nativen Host) herunter.	Auf der von Ihnen erstellten VM ist die Windows-Firewall deaktiviert. Außerdem ist kein Virenschutz installiert. Daher wird empfohlen, die Programme und Komponenten zuerst auf den nativen Host herunterzuladen und dann auf die VM in VMware Workstation zu kopieren.
Schritt 47: Extrahieren Sie "sigcheck.zip" an folgendem Speicherort: `C:\WINDOWS\system32`.	
Schritt 48: Navigieren Sie in Windows Explorer zu C:\WINDOWS\system32, und doppelklicken Sie auf **sigcheck.exe**.	
Schritt 49: Klicken Sie in der Warnmeldung auf **Ausführen**, wenn Sie dazu aufgefordert werden.	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

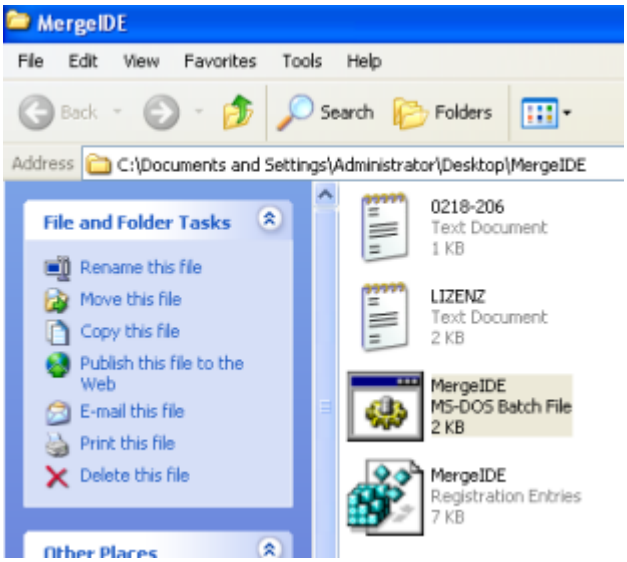
Schritt	Details
Schritt 50: Klicken Sie im **Sigcheck License Agreement** (Sigcheck-Lizenzvertrag) auf **Agree** (Ich stimme zu). Nach dem Klicken auf **Agree** (Ich stimme zu) wird keine Bestätigungsmeldung angezeigt.	
Schritt 51: Laden Sie die ZIP-Datei "MergeIDE.zip" von der Seite https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip auf den nativen Computer herunter, und kopieren Sie sie auf die VM.	
Schritt 52: Extrahieren Sie MergeIDE.zip, und führen Sie die MergeIDE-Batchdatei auf der VM aus.	• Klicken Sie in der Warnmeldung auf **Ausführen**, wenn Sie dazu aufgefordert werden. • Schließen Sie Windows Explorer.
Schritt 53: Deaktivieren Sie Windows-Updates.	1 Wählen Sie **Start** | **Einstellungen** | **Systemsteuerung**. 2 Öffnen Sie **System**. 3 Deaktivieren Sie auf der Registerkarte **Automatische Updates** die Option **Den Computer auf dem neusten Stand halten**. 4 Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

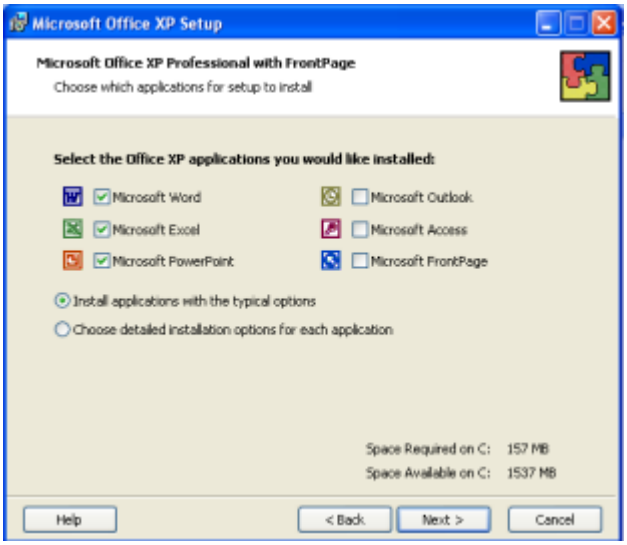
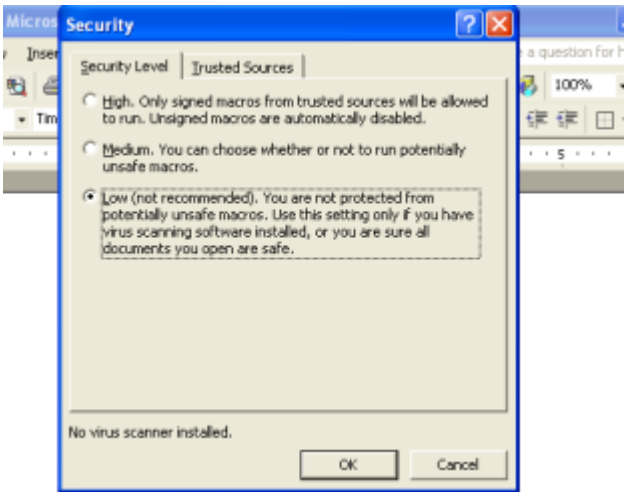
Schritt	Details
Schritt 54: Um Microsoft Word-, Excel- und PowerPoint-Dateien zu analysieren, installieren Sie Microsoft Office 2003 auf dem virtuellen Computer.	
Schritt 55: Senken Sie die Sicherheitsstufe, um Makros für Office-Anwendungen auszuführen.	• Öffnen Sie Microsoft Word 2003, und wählen Sie **Extras** | **Makro** | **Sicherheit** und dann **Niedrig**, und klicken Sie auf **OK**.  • Setzen Sie genauso die Makrosicherheit für Microsoft Excel und PowerPoint herab.

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

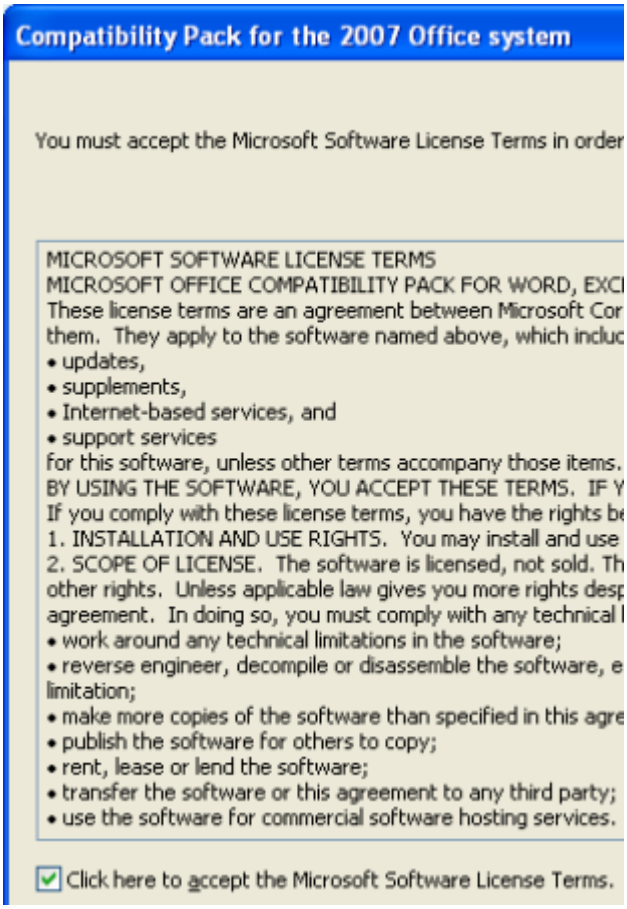
Schritt	Details
Schritt 56: Sie benötigen das Compatibility Pack, um Microsoft Office-Dateien öffnen zu können, die mit einer neueren Version von Microsoft Office erstellt wurden. Beispiel: Zum Öffnen einer DOCX-Datei mit Office 2003 muss das entsprechende Compatibility Pack installiert sein. Rufen Sie http://www.microsoft.com/en-us/download/details.aspx?id=3 auf, und laden Sie das erforderliche Microsoft Office Compatibility Pack für Word-, Excel- und PowerPoint-Dateiformate herunter. Installieren Sie es anschließend auf dem virtuellen Computer.	
Schritt 57: Aktivieren Sie im Dialogfeld **Compatibility Pack für 2007 Office System** die Option **Klicken Sie hier, um den Microsoft-Software-Lizenzbedingungen zuzustimmen**, und klicken Sie auf **OK**.	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

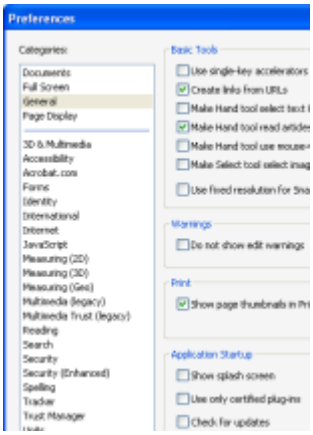
Schritt	Details
Schritt 58: Um PDF-Dateien zu analysieren, laden Sie Adobe Reader auf den nativen Host herunter, und kopieren Sie ihn auf die VM. In diesem Beispiel wird Adobe Reader 9.0 verwendet.	1 Installieren Sie Adobe Reader 9.0 auf der VM. 2 Öffnen Sie Adobe Reader, und klicken Sie auf **Akzeptieren**.  3 Wählen Sie in Adobe Reader **Bearbeiten** | **Voreinstellungen** | **Allgemein** , und deaktivieren Sie **Nach Updates suchen**. 
Schritt 59: Laden Sie die folgenden Programme auf den nativen Host herunter, und installieren Sie sie auf der VM.	1 Laden Sie Microsoft Visual C++ 2005 Redistributable Package (x86) von der Seite http://www.microsoft.com/en-us/download/details.aspx?id=3387 herunter,und installieren Sie das Programm. 2 Laden Sie Microsoft Visual C++ 2008 Redistributable Package (x86) von der Seite http://www.microsoft.com/en-us/download/details.aspx?id=5582 herunter,und installieren Sie das Programm. 3 Laden Sie Microsoft Visual C++ 2010 Redistributable Package (x86) von der Seite http://www.microsoft.com/en-us/download/details.aspx?id=5555 herunter,und installieren Sie das Programm. 4 Laden Sie Microsoft .NET Framework 2.0 Service Pack 2 (x86-Version) von der Seite http://www.microsoft.com/en-us/download/details.aspx?id=1639 herunter,und installieren Sie das Programm.

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

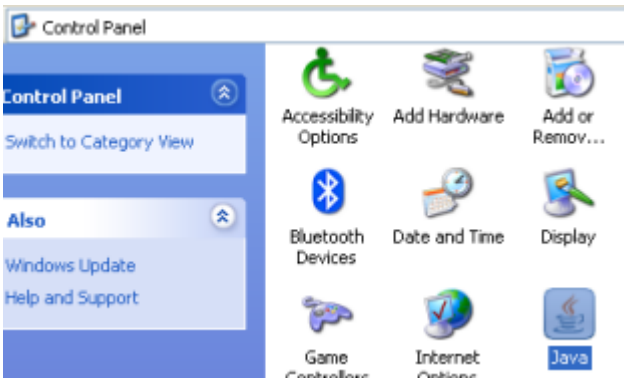
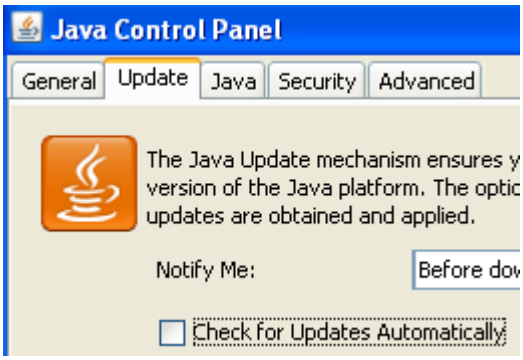
Schritt	Details
Schritt 60: Laden Sie zum Analysieren von JAR-Dateien Java Runtime Environment herunter, und installieren Sie die Anwendung. In diesem Beispiel wird Java 7 Update 25 verwendet.	
Schritt 61: Öffnen Sie Java in der Systemsteuerung.	
Schritt 62: Deaktivieren Sie auf der Registerkarte **Update** die Option **Automatisch nach Updates suchen.**	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

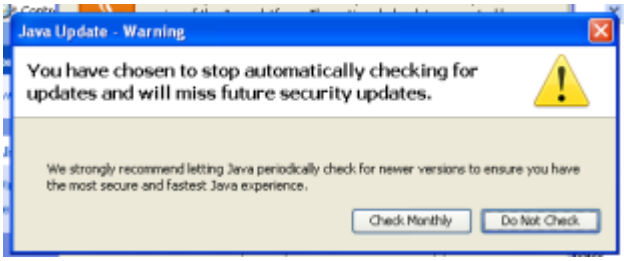
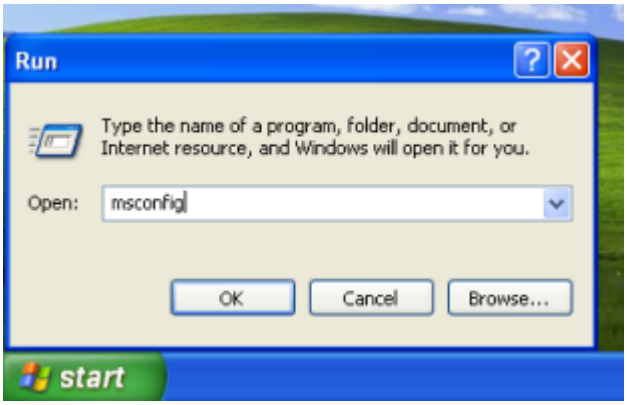
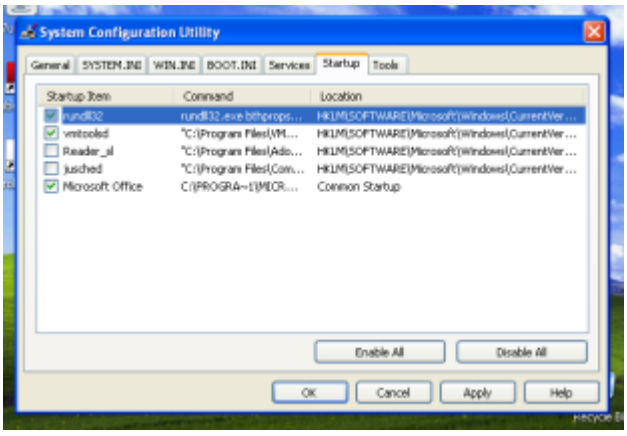
Schritt	Details
Schritt 63: Wählen Sie im Dialogfeld "Java-Update – Warnung" die Option **Nicht überprüfen**, und klicken Sie dann in der Java-Systemsteuerung auf **OK**.	
Schritt 64: Geben Sie im Windows-Dialogfeld "Ausführen" `msconfig` ein.	
Schritt 65: Navigieren Sie im Systemkonfigurationsprogramm zur Registerkarte **Start**.	 Deaktivieren Sie *reader_sl* und *jusched*, und klicken Sie dann auf **OK**.

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

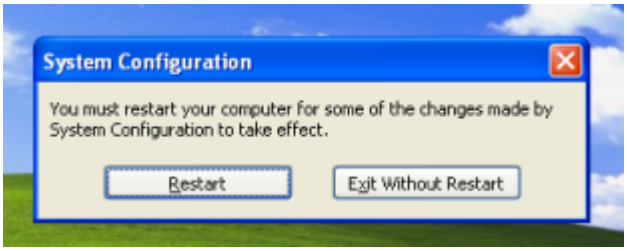
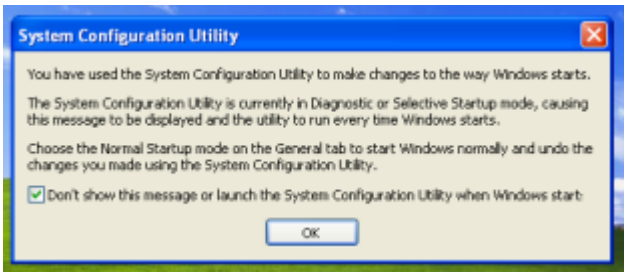
Schritt	Details
Schritt 66: Klicken Sie in der **Systemkonfiguration** auf **Neu starten**.	
Schritt 67: Aktivieren Sie im Dialogfeld **Systemkonfigurationsprogramm** das Kontrollkästchen **Meldung nicht mehr anzeigen und dieses Programm beim Windows-Start nicht mehr starten**, und klicken Sie auf **OK**.	

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

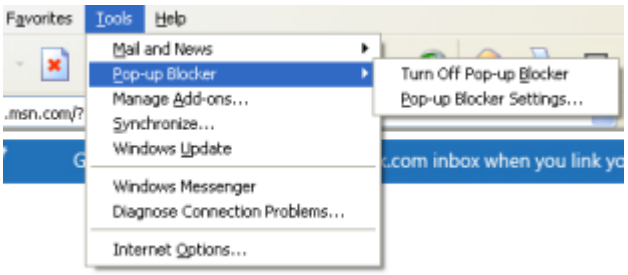
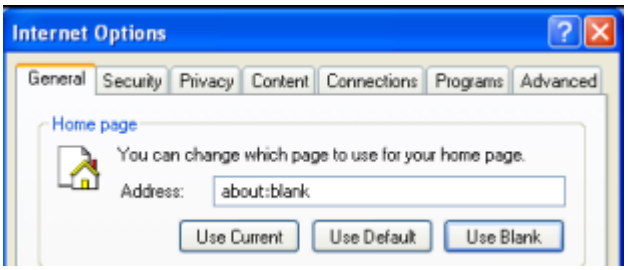
Schritt	Details
Schritt 68: Öffnen Sie den Standard-Browser, und richten Sie ihn für Malware-Analysen ein. In diesem Beispiel wird Internet Explorer verwendet.	1 Stellen Sie sicher, dass der Popupblocker eingeschaltet ist. Wählen Sie in Internet Explorer **Extras** | **Popupblocker** | **Popupblocker einschalten**.  2 Wählen Sie **Extras** | **Internetoptionen** , und wählen Sie abhängig von der Version von Internet Explorer unter **Startseite** entweder **Leere Seite** oder **Neue Registerkarte** aus.  3 Wechseln Sie zur Registerkarte **Erweitert**, und suchen Sie **Sicherheit**. 4 Wählen Sie **Ausführung aktiver Inhalte in Dateien auf dem lokalen Computer zulassen** aus.

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

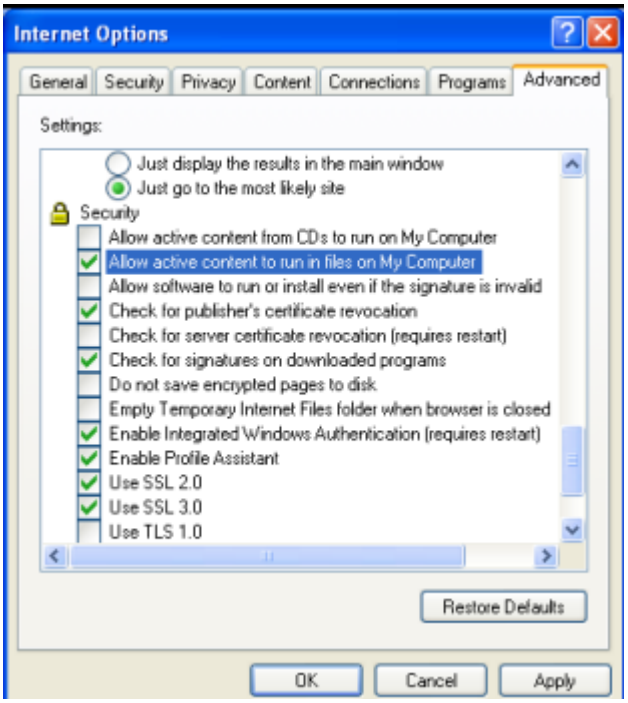
Schritt	Details
	 **5** Klicken Sie auf **OK**.

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

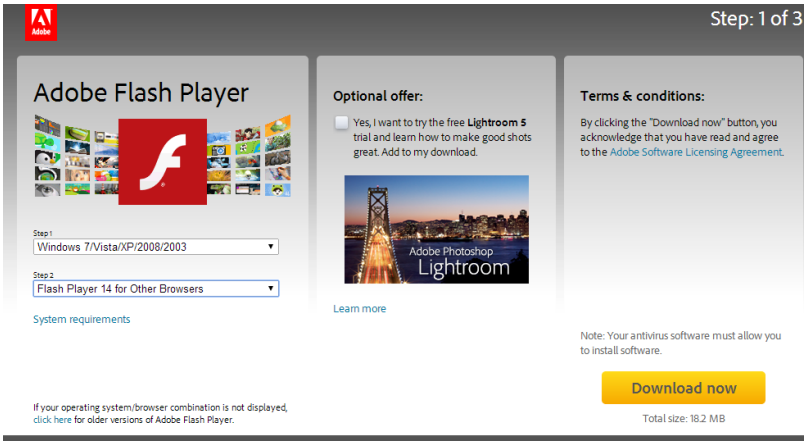
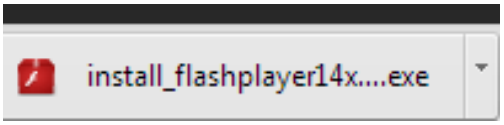
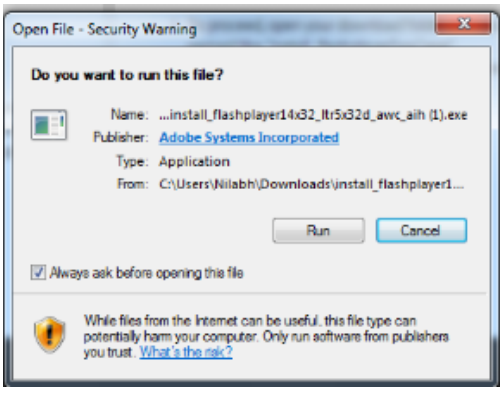
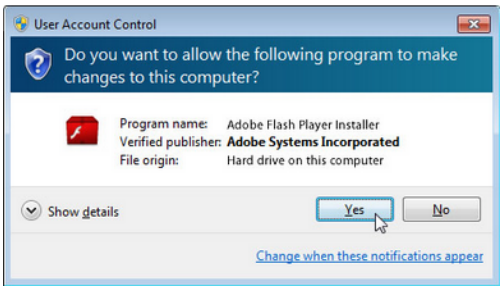
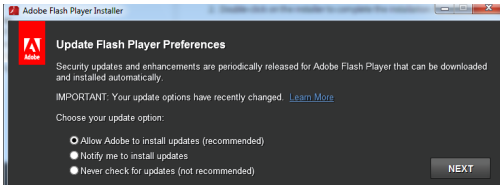
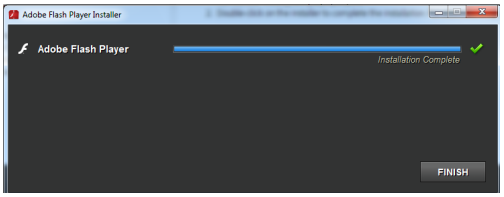
Schritt	Details
Schritt 69: Um eine Flash-Datei (SWF) dynamisch zu analysieren, installieren Sie die erforderliche Version von Adobe Flash. In diesem Beispiel wird Flash Player 14 verwendet.	1 Rufen Sie http://get.adobe.com/de/flashplayer/otherversions/ auf. 2 Wählen Sie gemäß Ihren Anforderungen ein Betriebssystem und eine Flash Player-Version in den Dropdown-Menüs **Schritt 1** und **Schritt 2** aus (siehe unten). 3 Klicken Sie auf **Jetzt herunterladen**.  4 Doppelklicken Sie in der unteren Ecke Ihres Bildschirms auf die Installationsdatei für Adobe Flash Player **(install_flashplayer xxx.exe)**.  5 Klicken Sie im Dialogfeld **Sicherheitswarnung** auf **Ausführen**.  6 Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.

Tabelle 5-2 Erstellen Sie eine VMDK-Datei aus einem ISO-Image von Windows XP SP2 oder SP3. *(Fortsetzung)*

Schritt	Details
	 7 Wählen Sie Ihre Aktualisierungsoption, und klicken Sie auf **WEITER**.  8 Klicken Sie auf **FERTIGSTELLEN**, um die Adobe Flash Player-Installation abzuschließen. 
Schritt 70: Fahren Sie das virtualMachineImage herunter, indem Sie folgende Optionen auswählen: **Start** | **Herunterfahren.**	
Schritt 71: Navigieren Sie zu dem Speicherort, den Sie in Schritt 8 angegeben haben, um die VMDK-Datei mit dem Namen `virtualMachineImage-flat.vmdk` aufzurufen.	

Erstellen einer VMDK-Datei für Windows 2003 Server

Bevor Sie beginnen

- Laden Sie VMware Workstation 9.0 oder höher von der Seite http://www.vmware.com/products/workstation/workstation-evaluation herunter, und installieren Sie das Programm.
- Stellen Sie sicher, dass Sie über ein ISO-Image von Windows 2003 SP1 bzw. SP2 verfügen, für das Sie die VMDK-Datei erstellen. Nur Windows 2003 Server Enterprise Edition wird unterstützt.
- Stellen Sie sicher, dass Sie über den Lizenzschlüssel für das Betriebssystem verfügen.

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2

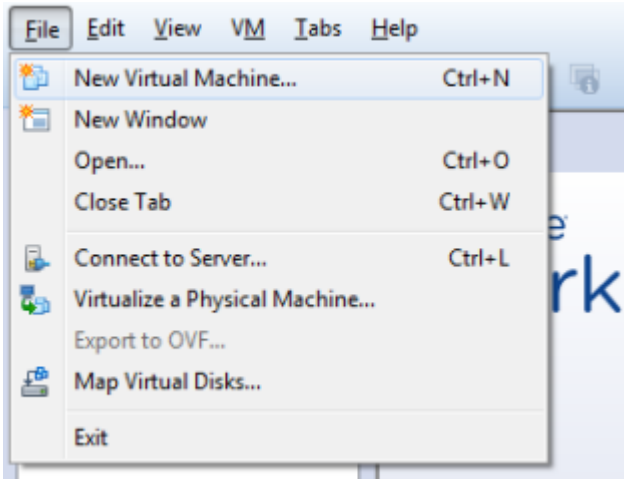
Schritt	Details
Schritt 1: Starten Sie VMware Workstation.	In diesem Beispiel wird VMware Workstation 10 verwendet.
Schritt 2: Wählen Sie auf der VMware Workstation-Seite **Datei** | **New Virtual Machine (Neuer virtueller Computer)**.	
Schritt 3: Wählen Sie im Fenster **New Virtual Machine Wizard** (Assistent für neue virtuelle Computer) die Option **Custom (Advanced)** (Benutzerdefiniert (erweitert)), und klicken Sie auf **Next** (Weiter).	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

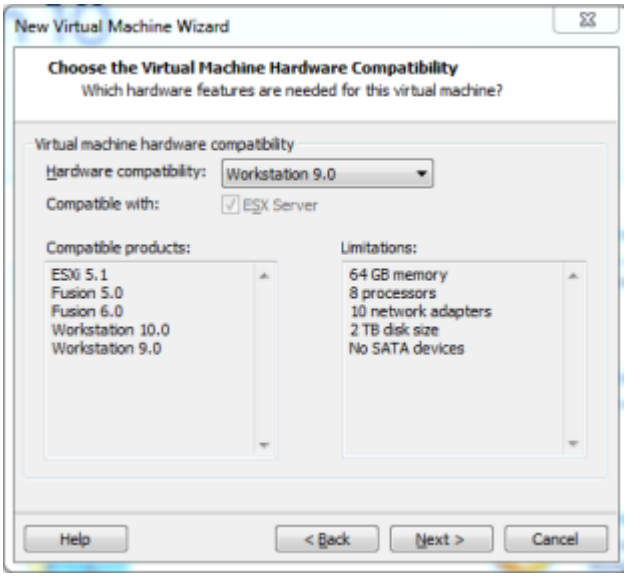
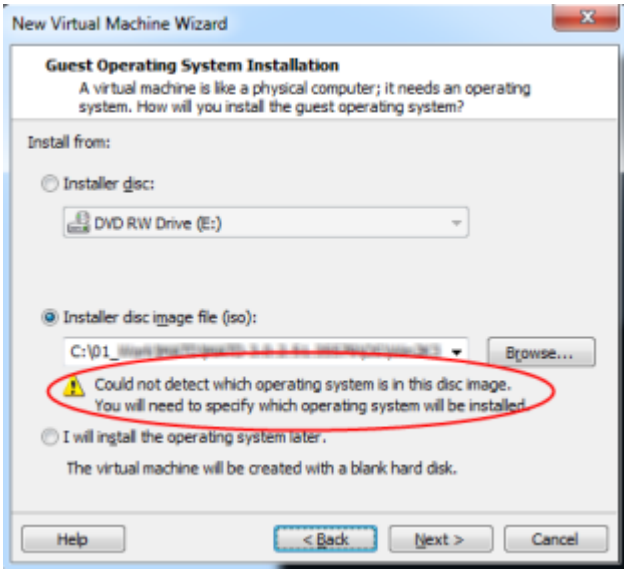
Schritt	Details
Schritt 4: Wählen Sie im Fenster **Choose the Virtual Machine Hardware Compatibility** (Wählen der Hardwarekompatibilität des virtuellen Computers) **Workstation 9.0** aus der Dropdown-Liste **Hardware compatibility** (Hardwarekompatibilität) aus. Akzeptieren Sie bei den anderen Feldern die Standardwerte, und klicken Sie auf **Next** (Weiter).	
Schritt 5: Wählen Sie im Fenster **Guest Operating System Installation** (Installation eines Gast-Betriebssystems) entweder **Installer disc** (Installationsdatenträger) oder **Installer disc image file (iso)** (Image-Datei des Installationsdatenträgers), navigieren Sie zum ISO-Image, wählen Sie es aus, und klicken Sie anschließend auf **Next** (Weiter).	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

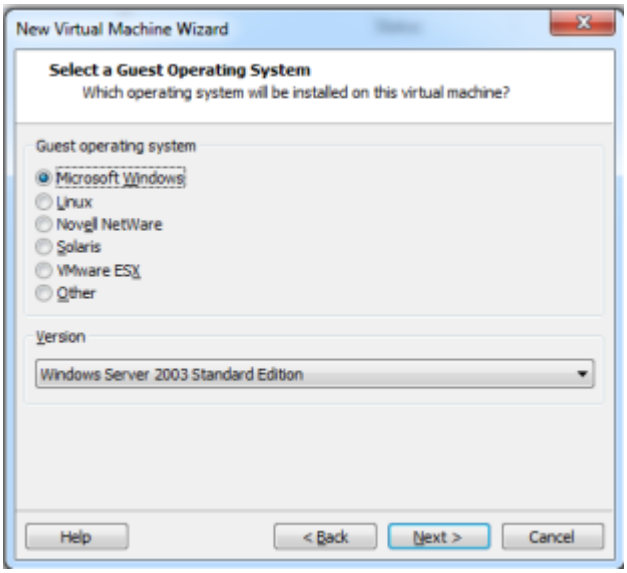
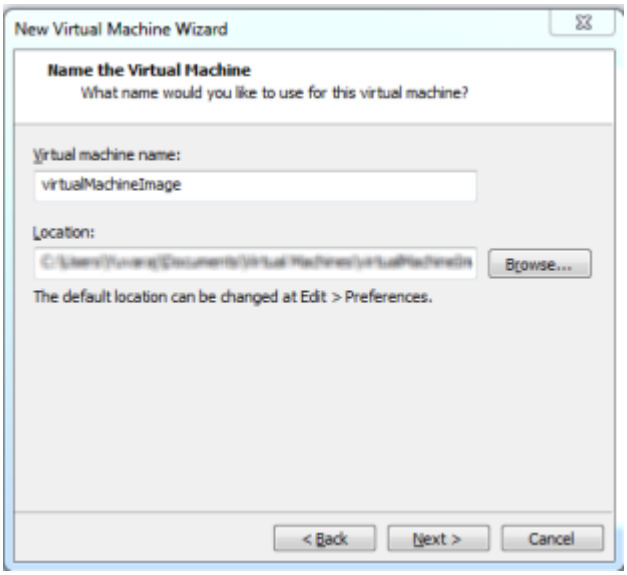
Schritt	Details
Schritt 6: Wählen Sie im Fenster **Select a Guest Operating System** (Wählen des Gast-Betriebssystems) die entsprechende Version.	
Schritt 7: Geben Sie die Informationen im Fenster **Name the Virtual Machine** (Benennen des virtuellen Computers) ein, und klicken Sie anschließend auf **Next** (Weiter).	• **Virtual Machine name** (Name des virtuellen Computers) – Geben Sie `virtualMachineImage` als Namen ein. • **Location** (Speicherort) – Navigieren Sie zu dem Ordner, in dem die VDMK-Datei erstellt werden soll, und wählen Sie ihn aus. 

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

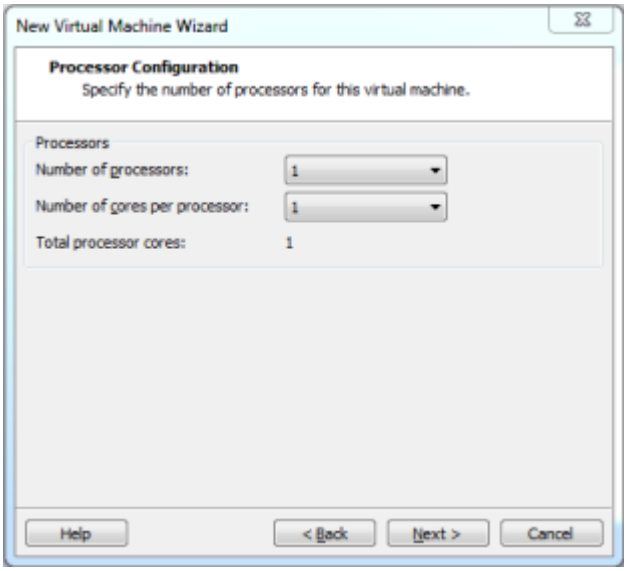
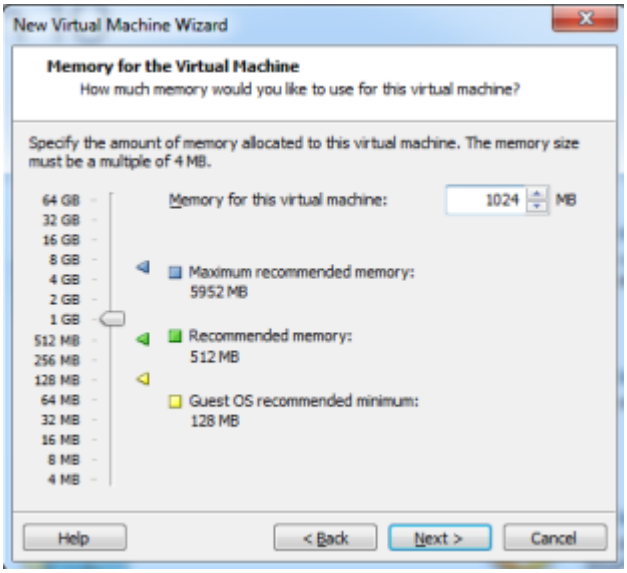
Schritt	Details
Schritt 8: Übernehmen Sie im Fenster **Processor Configuration** (Prozessorkonfiguration) die Standardwerte, und klicken Sie auf **Next** (Weiter).	
Schritt 9: Legen Sie im Fenster **Memory for the Virtual Machine** (Speicher für den virtuellen Computer) 1.024 MB als Speicher fest.	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

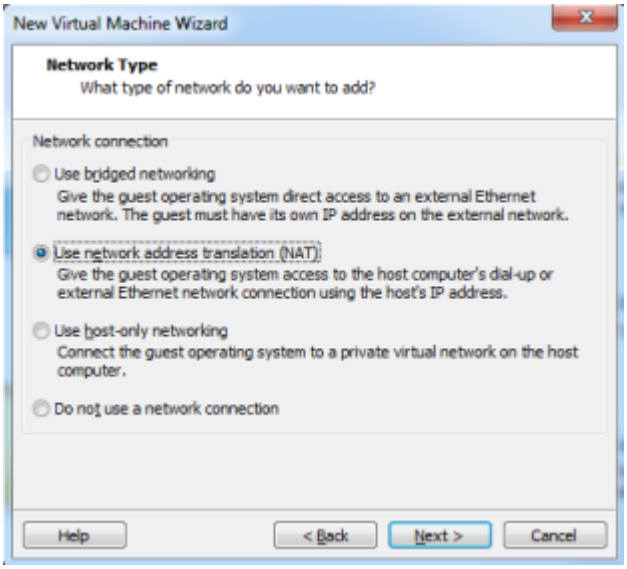
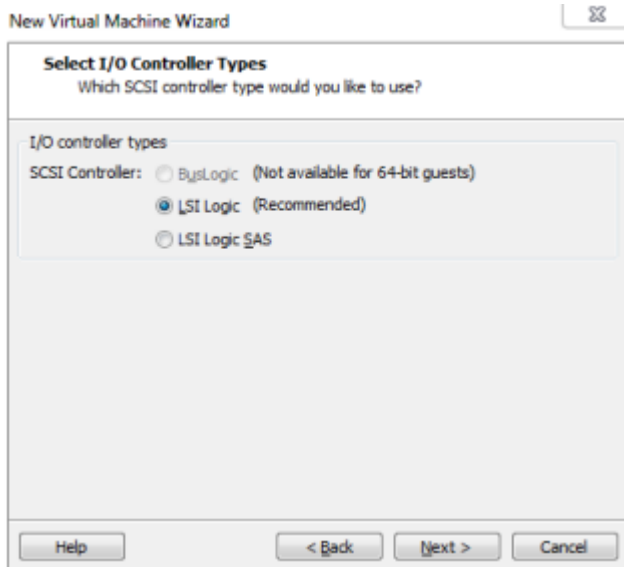
Schritt	Details
Schritt 10: Übernehmen Sie im Fenster **Network Type** (Netzwerktyp) die Standardauswahl.	
Schritt 11: Übernehmen Sie unter **Select I/O Controller Types** (Auswählen der I/O-Controller-Typen) die Standardauswahl.	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

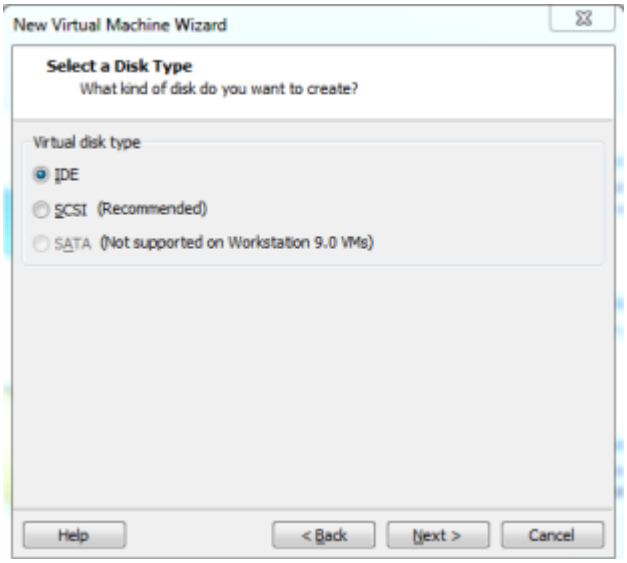
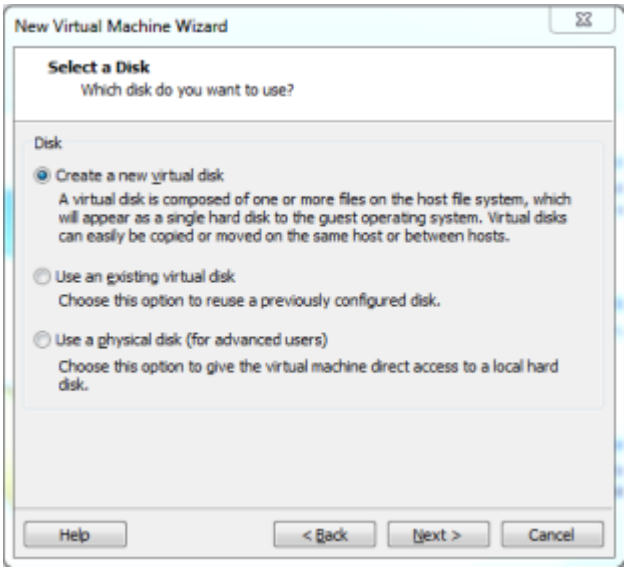
Schritt	Details
Schritt 12: Wählen Sie auf der Seite **Auswählen eines Datenträgertyps** die Option **IDE**, und klicken Sie auf **Next** (Weiter). SCSI-Datenträger sind mit McAfee Advanced Threat Defense nicht kompatibel.	
Schritt 13: Wählen Sie im Fenster **Auswählen eines Datenträgers** die Option **Create a new virtual disk** (Neuen virtuellen Datenträger erstellen), und klicken Sie auf **Next** (Weiter).	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

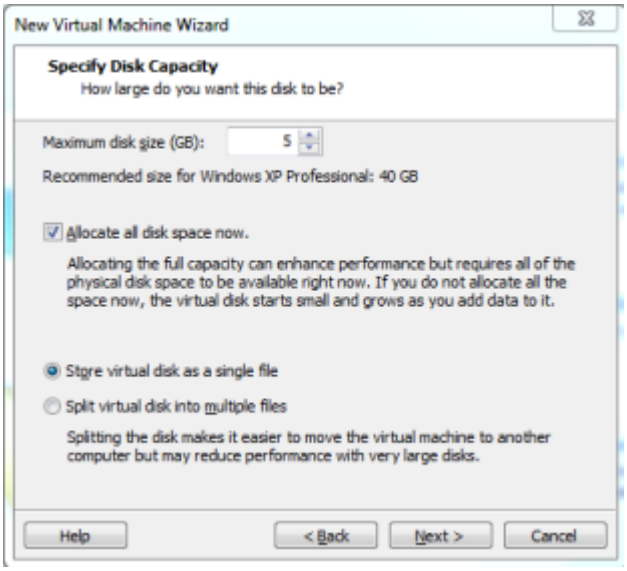
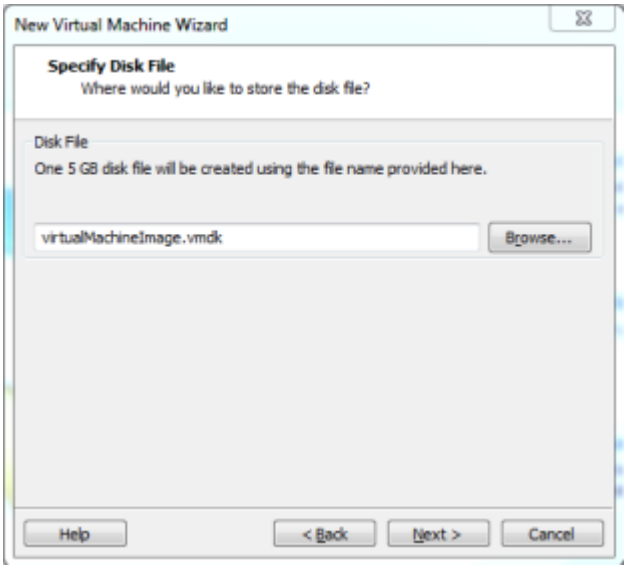
Schritt	Details
Schritt 14: Geben Sie die Details im Fenster **Angeben der Speicherkapazität** an, und klicken Sie auf **Next** (Weiter).	• **Maximum disk size (GB)** (Maximale Datenträgergröße in GB) – Geben Sie 5 GB an. • Wählen Sie **Allocate all disk space now** (Sämtlichen Speicherplatz jetzt zuweisen). • Wählen Sie **Store virtual disk as a single file** (Virtuellen Datenträger als einzelne Datei speichern). 
Schritt 15: Vergewissern Sie sich, dass im Fenster **Specify Disk file** (Datenträgerdatei angeben) standardmäßig "virtualMachineImage.vmdk" angezeigt wird, und klicken Sie auf **Next** (Weiter). Wenn Sie unter **Virtual Machine name** (Name des virtuellen Computers) einen anderen Namen angegeben haben, wird dieser hier angezeigt.	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

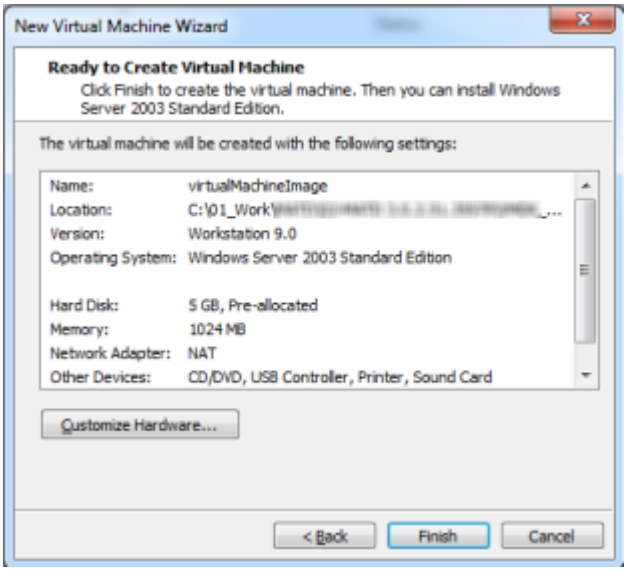
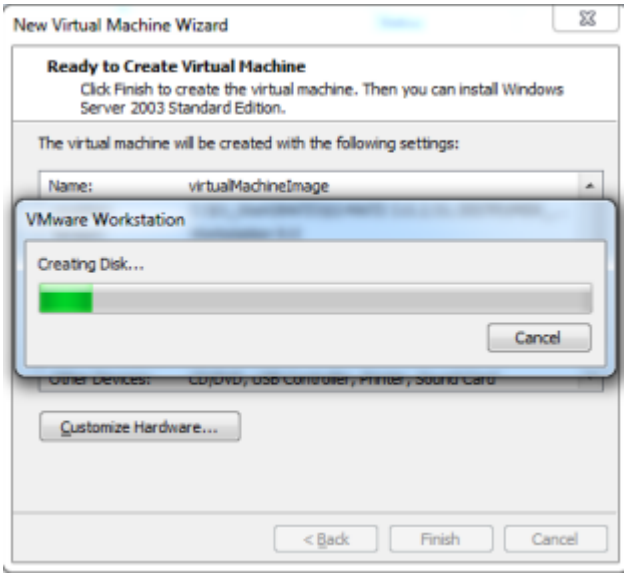
Schritt	Details
Schritt 16: Überprüfen Sie die Einstellungen für das Erstellen des virtuellen Computers, und klicken Sie auf **Finish** (Fertig stellen). Dadurch wird der virtuelle Computer erstellt. Anschließend müssen Sie das Betriebssystem installieren.	 

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

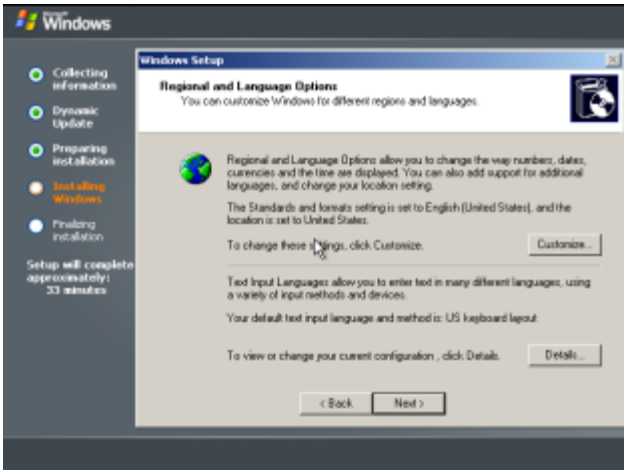
Schritt	Details
Schritt 17: Schalten Sie in der VMware Workstation den zuvor erstellten virtuellen Computer ein, und installieren Sie Windows Server 2003, indem Sie die üblichen Schritte ausführen. • Dieser Schritt kann etwa 30 Minuten in Anspruch nehmen. • Sie können während der Installation die Partition mit dem NTFS-Dateisystem formatieren. • Installieren Sie nicht VMware Tools. Wenn Sie die Installation von VMware Tools nicht angehalten haben, können Sie dennoch mit der VMDK-Dateierstellung fortfahren. Das Programm muss aber deinstalliert sein, sobald die VMDK-Datei bereit ist.	
Schritt 18: Im Fenster **Regions- und Sprachoptionen** können Sie die Einstellungen anpassen.	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

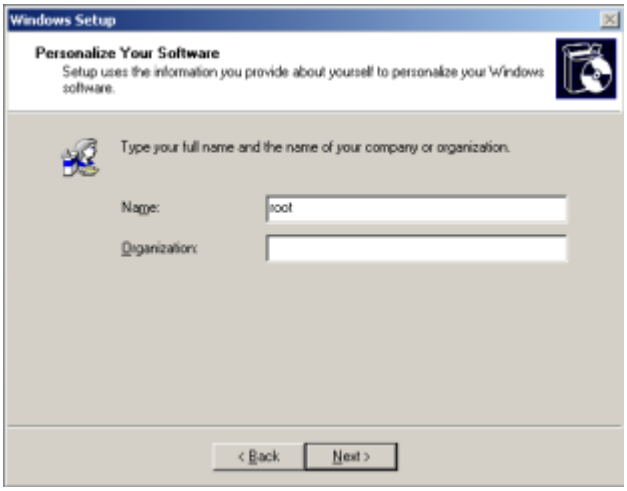
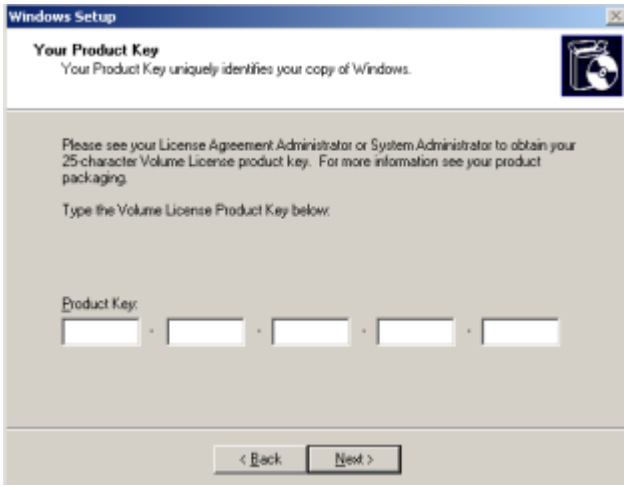
Schritt	Details
Schritt 19: Geben Sie die folgenden Details im Fenster **Windows Setup** ein.	• **Name:** Geben Sie `root` ein. • **Organisation:** Lassen Sie dieses Feld leer, und klicken Sie auf **Weiter**. 
Schritt 20: Geben Sie einen Produktschlüssel ein, und klicken Sie auf **Weiter**.	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

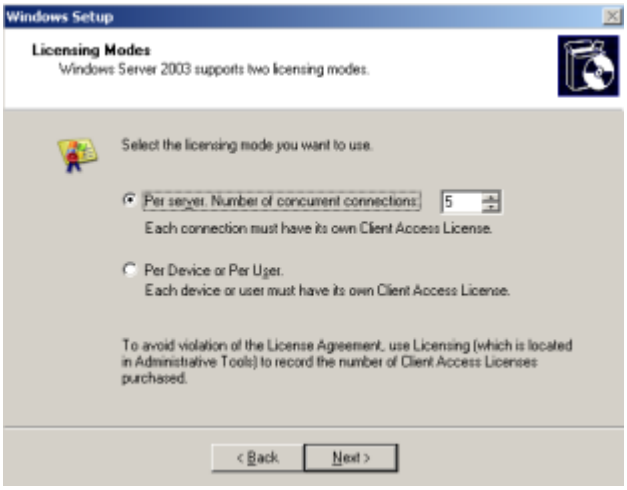
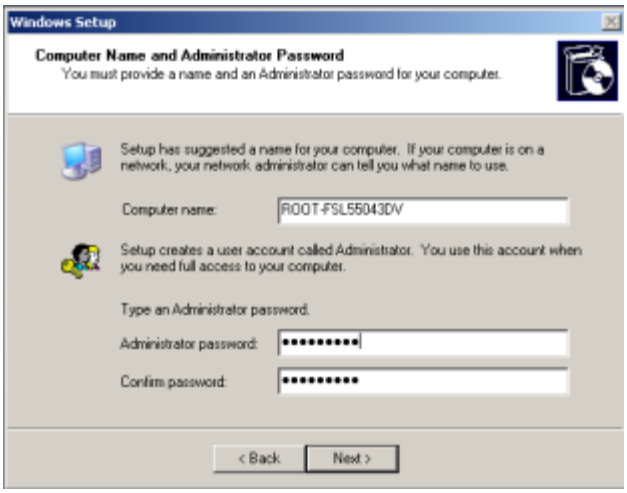
Schritt	Details
Schritt 21: Wählen Sie das Lizenzmodell **Pro Server**, und geben Sie die gültige Anzahl gleichzeitiger Verbindungen pro Lizenz ein.	
Schritt 22: Geben Sie die folgenden Details im Fenster **Computername und Administratorkennwort** ein.	• Computername – Akzeptieren Sie den Standardwert. • Administratorkennwort – `cr@cker42` • Kennwort bestätigen – `cr@cker42` 

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

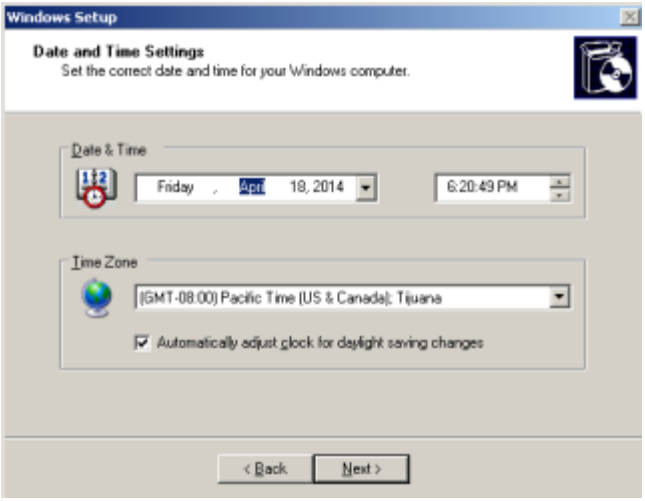
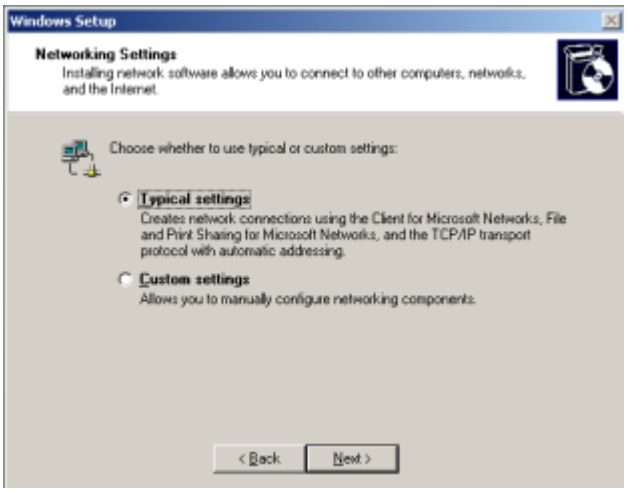
Schritt	Details
Schritt 23: Klicken Sie im Fenster **Datums- und Uhrzeiteinstellungen** auf **Weiter**.	
Schritt 24: Übernehmen Sie im Fenster **Netzwerkeinstellungen** die Standardwerte, und klicken Sie auf **Weiter**.	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

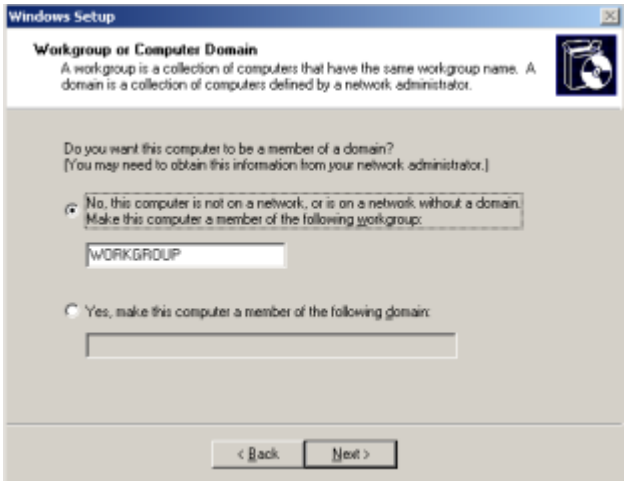
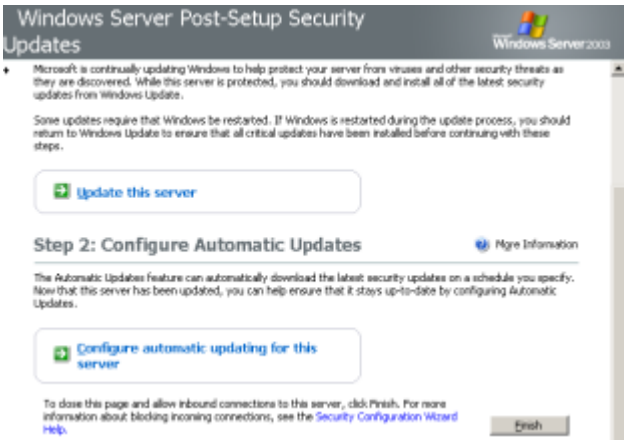
Schritt	Details
Schritt 25: Übernehmen Sie im Fenster **Arbeitsgruppe oder Computerdomäne** die Standardwerte, und klicken Sie auf **Weiter**.	
Schritt 26: Melden Sie sich mit den folgenden Anmeldeinformationen beim virtuellen Computer an.	• **User** (Benutzer): `administrator` • **Password** (Kennwort): `cr@cker42`
Schritt 27: Wenn die Seite **Sicherheitsupdatekonfiguration für Windows Server** angezeigt wird, klicken Sie auf **Fertig stellen**.	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

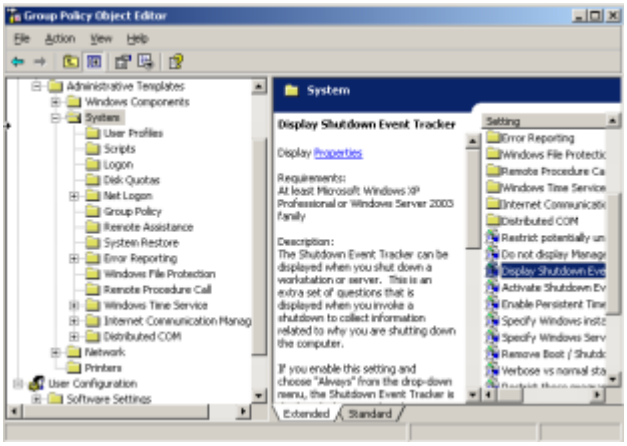
Schritt	Details
Schritt 28: Wenn das Fenster **Serververwaltung** angezeigt wird, aktivieren Sie das Kontrollkästchen **Diese Seite bei der Anmeldung nicht anzeigen**, und schließen Sie das Fenster.	
Schritt 29: Führen Sie die folgenden Schritte aus.	1 Wählen Sie **Start** | **Ausführen** , und geben Sie `gpedit.msc` ein. 2 Wählen Sie im Fenster **Gruppenrichtlinienobjekt-Editor** die Optionen **Computerkonfiguration** | **Administrative Vorlagen** | **System** , und doppelklicken Sie auf **Ereignisprotokollierung für Herunterfahren anzeigen**.  3 Wählen Sie **Deaktiviert**, und klicken Sie auf **OK**. 4 Schließen Sie das Fenster **Gruppenrichtlinienobjekt-Editor**.
Schritt 30: Führen Sie die folgenden Schritte für Windows Server 2003 SP1 aus. Für Windows Server 2003 SP2 führen Sie diesen Schritt nicht aus.	1 Rufen Sie http://support.microsoft.com/hotfix/KBHotfix.aspx?kbnum=899260&kbln=en-us auf, und installieren Sie den HotFix für Ihre Version von Windows Server 2003. 2 Starten Sie den Computer neu. 3 Geben Sie in der Windows-Eingabeaufforderung `tlntsvr /service` ein, und drücken Sie die Eingabetaste.

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

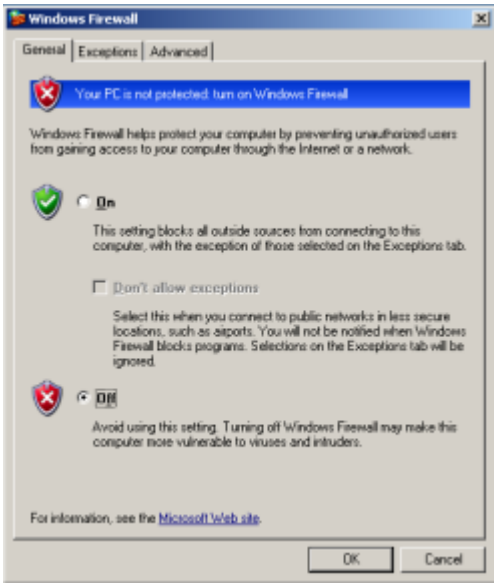
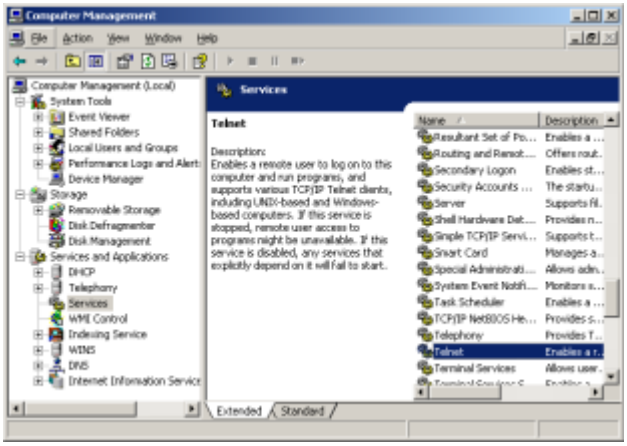
Schritt	Details
Schritt 31: Wählen Sie im virtualMachineImage die Optionen **Start** | **Systemsteuerung** | **Windows-Firewall** | **AUS.**	
Schritt 32: Klicken Sie auf **Start** und dann mit der rechten Maustaste auf **Arbeitsplatz.** Wählen Sie dann **Verwalten** | **Dienste und Anwendungen** | **Dienste.** Doppelklicken Sie anschließend auf **Telnet.**	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

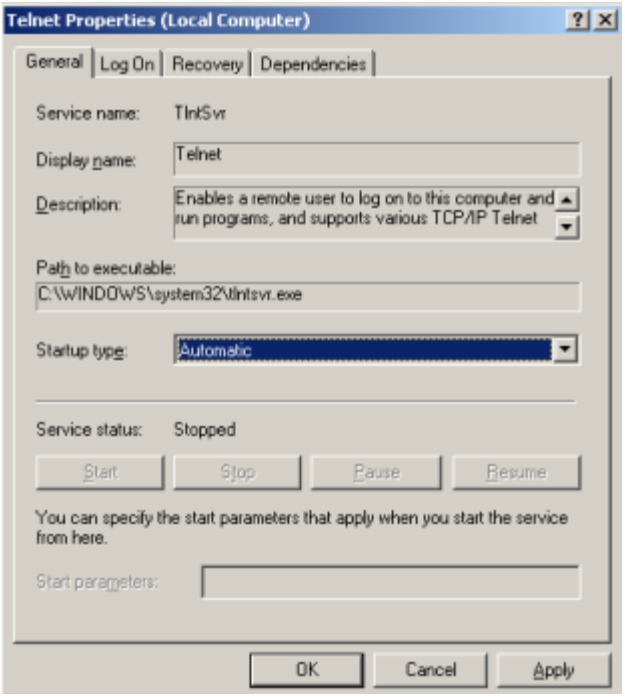
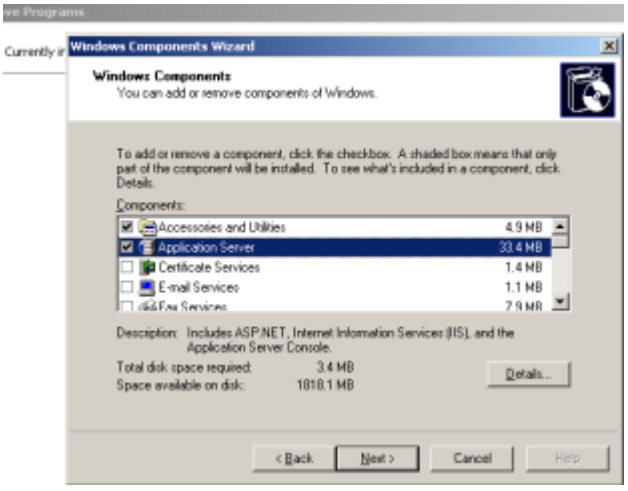
Schritt	Details
Schritt 33: Wählen Sie im Fenster **Eigenschaften von Telnet (Lokaler Computer)** aus der Dropdown-Liste **Starttyp** die Option **Automatisch.** Wählen Sie dann **Übernehmen** | **Start** | **OK.**	
Schritt 34: Aktivieren Sie FTP auf der VM.	1 Wählen Sie im virtualMachineImage die Optionen **Start** | **Systemsteuerung** | **Software** | **Windows-Komponenten hinzufügen/entfernen.**  2 Doppelklicken Sie auf **Anwendungsserver.** 3 Doppelklicken Sie auf **Internetinformationsdienste (IIS).**

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

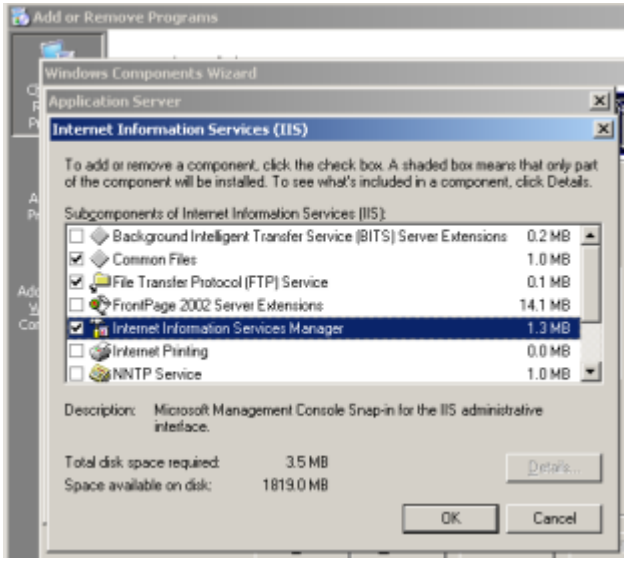
Schritt	Details
Schritt 35: Führen Sie im Popupfenster **Internetinformationsdienste (IIS)** die folgenden Schritte aus.	1 Wählen Sie **Gemeinsame Dateien**. 2 Wählen Sie **FTP-Dienst (File Transfer Protocol)**. 3 Wählen Sie **Internetinformationsdienste-Manager**, klicken Sie auf **OK** und anschließend im **Assistenten für Windows-Komponenten** auf **Weiter**. 

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

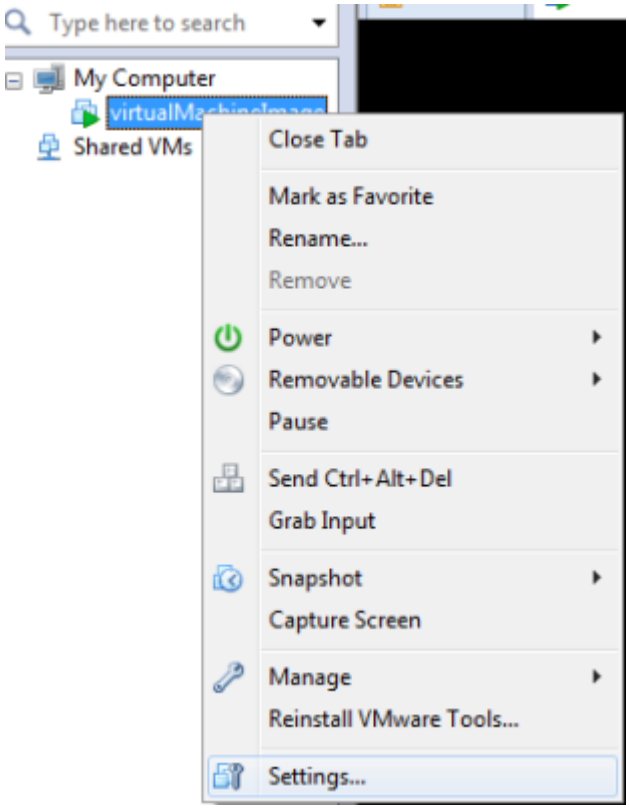
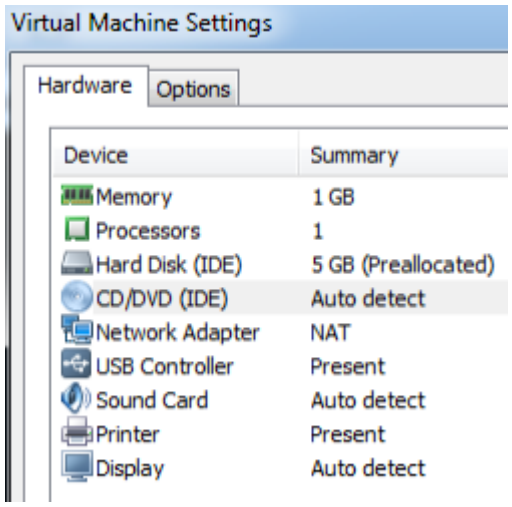
Schritt	Details
Schritt 36: Klicken Sie in VMware Workstation mit der rechten Maustaste auf die VM, in diesem Beispiel "virtualMachineImage". Wählen Sie dann **Settings** (Einstellungen) aus.	
Schritt 37: Wählen Sie im Fenster "Einstellungen des virtuellen Computers" den Eintrag **CD/DVD (IDE)** aus.	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

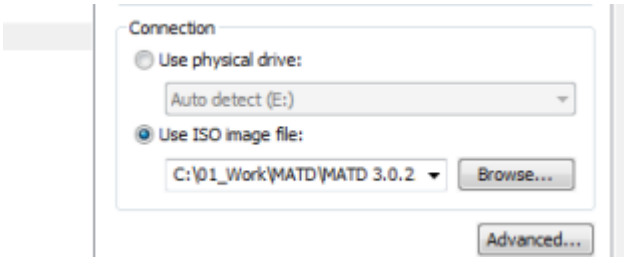
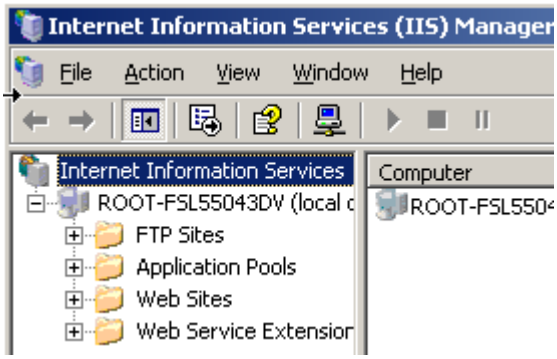
Schritt	Details
Schritt 38: Navigieren Sie im Feld **Use ISO image file** (ISO-Image-Datei verwenden) zum ISO-Image, das Sie verwendet haben, und klicken Sie auf **OK**. Schließen Sie Windows Explorer, falls dieser geöffnet wird.	
Schritt 39: Wählen Sie im virtualMachineImage die Optionen **Start** | **Systemsteuerung** | **Verwaltung** | **Internetinformationsdienste (IIS).**	
Schritt 40: Erweitern Sie im Fenster **Internetinformationsdienste (IIS)** den Eintrag **Internetinformationsdienste.**	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

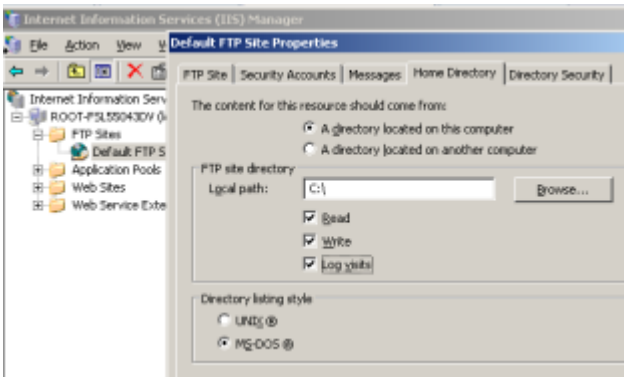
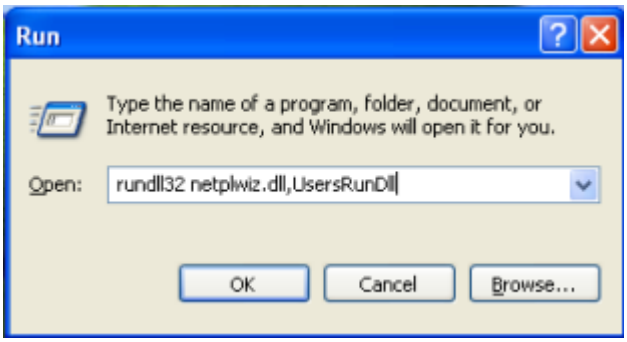
Schritt	Details
Schritt 41: Führen Sie die folgenden Schritte aus.	1 Wählen Sie **FTP-Sites**, und klicken Sie dann mit der rechten Maustaste auf **Standard-FTP-Site**. 2 Wählen Sie **Eigenschaften** | **Basisverzeichnis**. 3 Navigieren Sie zu C:\ 4 Wählen Sie **Lesen**. 5 Wählen Sie **Schreiben**. 6 Wählen Sie **Besuche protokollieren**, und klicken Sie auf **Übernehmen** und anschließend auf **OK**. 
Schritt 42: Richten Sie die automatische Anmeldung ein, indem Sie **Start** | **Ausführen**auswählen, `rundll32 netplwiz.dll,UsersRunDll` eingeben und die **Eingabetaste** drücken.	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

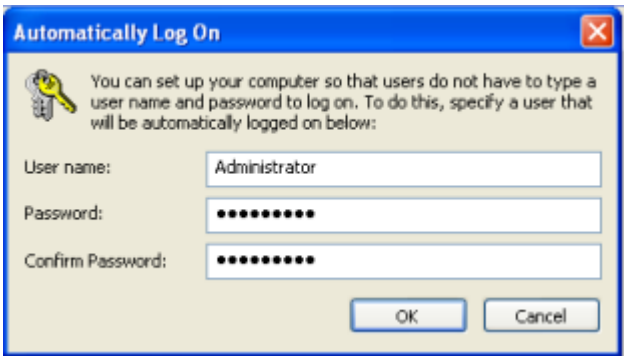
Schritt	Details
Schritt 43: Deaktivieren Sie im Fenster **Benutzerkonten** die Option **Benutzer müssen Benutzernamen und Kennwort eingeben**, und klicken Sie auf **Übernehmen**.	
Schritt 44: Führen Sie im Popupfenster **Automatische Anmeldung** die folgenden Schritte aus, und klicken Sie dann auf **OK**.	• **Benutzername** – Geben Sie `Administrator` ein. • **Kennwort** – Geben Sie `cr@cker42` ein. • **Kennwort bestätigen** – Geben Sie `cr@cker42` erneut ein. 
Schritt 45: Laden Sie Sigcheck von der Seite http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx auf Ihren Computer (den nativen Host) herunter.	Auf der von Ihnen erstellten VM ist die Windows-Firewall deaktiviert. Außerdem ist kein Virenschutz installiert. Daher wird empfohlen, die Programme und Komponenten zuerst auf den nativen Host herunterzuladen und dann auf die VM in VMware Workstation zu kopieren.

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

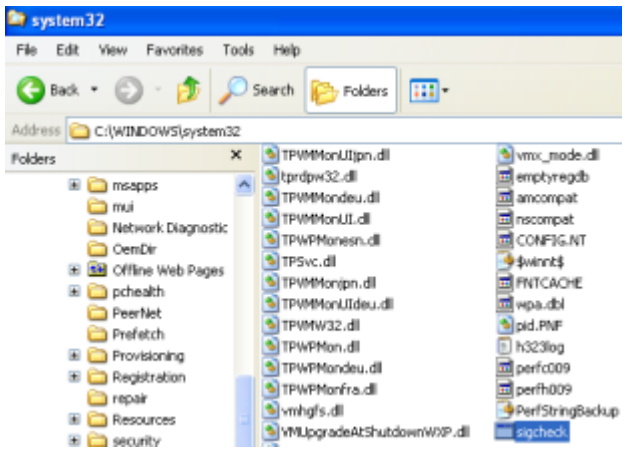
Schritt	Details
Schritt 46: Extrahieren Sie "sigcheck.zip" an folgendem Speicherort: `C:\WINDOWS\system32`.	 system32 File Edit View Favorites Tools Help Back Search Folders Address C:\WINDOWS\system32 Folders msapps mui Network Diagnostic OemDir Offline Web Pages pchealth PeerNet Prefetch Provisioning Registration repair Resources security TPVMMonUIJpn.dll tprdpw32.dll TPVMMondeu.dll TPVMMonUI.dll TPWPMonesn.dll TPSvc.dll TPVMMonJpn.dll TPVMMonUIdeu.dll TPVMW32.dll TPWPMon.dll TPWPMondeu.dll TPWPMonfra.dll vmhgfs.dll VMUpgradeAtShutdownWXP.dll vmx_mode.dll emptyregdb amcompat nscompat CONFIG.NT $winnt$ FNTCACHE wpa.dbl pid.PNF h323log perfc009 perfh009 PerfStringBackup sigcheck
Schritt 47: Navigieren Sie in Windows Explorer zu C:\WINDOWS\system32, und doppelklicken Sie auf **sigcheck.exe**.	
Schritt 48: Klicken Sie in der Warnmeldung auf **Ausführen**, wenn Sie dazu aufgefordert werden.	
Schritt 49: Klicken Sie im **Sigcheck License Agreement** (Sigcheck-Lizenzvertrag) auf **Agree** (Ich stimme zu). Nach dem Klicken auf **Agree** (Ich stimme zu) wird keine Bestätigungsmeldung angezeigt.	 SigCheck License Agreement You can also use the /accepteula command-line switch to accept the EULA. SYSINTERNALS SOFTWARE LICENSE TERMS These license terms are an agreement between Sysinternals (a wholly owned subsidiary of Microsoft Corporation) and you. Please read them. They apply to the software you are downloading from Systinternals.com, which includes the media on which you received it, if any. The terms also apply to any Sysinternals updates, supplements, Internet-based services, and Print Agree Decline

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

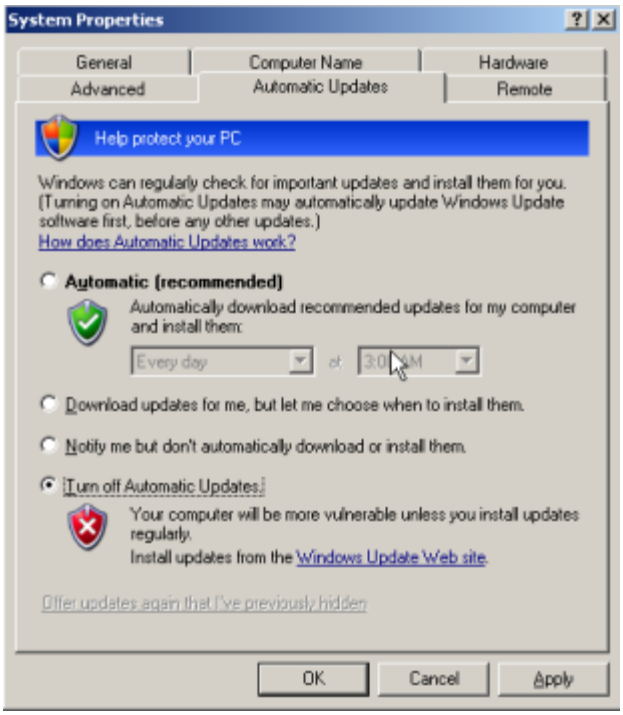
Schritt	Details
Schritt 50: Führen Sie die MergeIDE-Batchdatei auf der VM aus.	1 Laden Sie die ZIP-Datei "MergeIDE.zip" von der Seite https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip auf den nativen Computer herunter, und kopieren Sie sie auf die VM. 2 Extrahieren Sie die MergeIDE.zip, und führen Sie die MergeIDE-Batchdatei auf der VM aus. 3 Klicken Sie in der Warnmeldung auf **Ausführen**, wenn Sie dazu aufgefordert werden. 4 Schließen Sie Windows Explorer.
Schritt 51: Deaktivieren Sie Windows-Updates.	1 Wählen Sie **Start** | **Systemsteuerung** | **System** | **Automatische Updates.** 2 Aktivieren Sie im Fenster **Systemeigenschaften** die Option **Automatische Updates deaktivieren.**  3 Klicken Sie auf **Übernehmen** und anschließend auf **OK**.

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

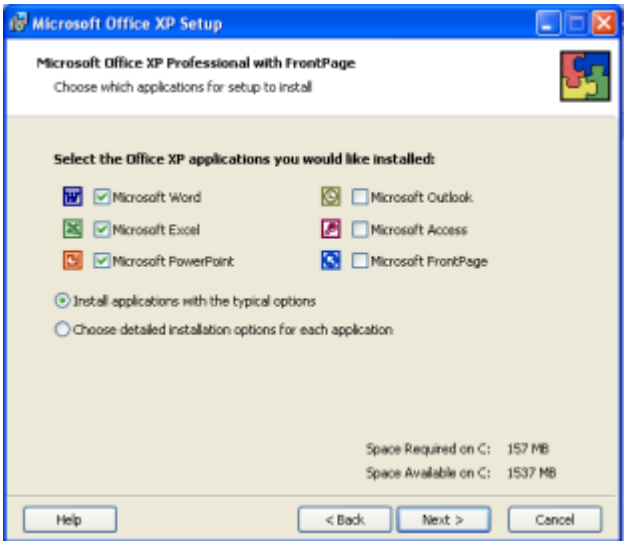
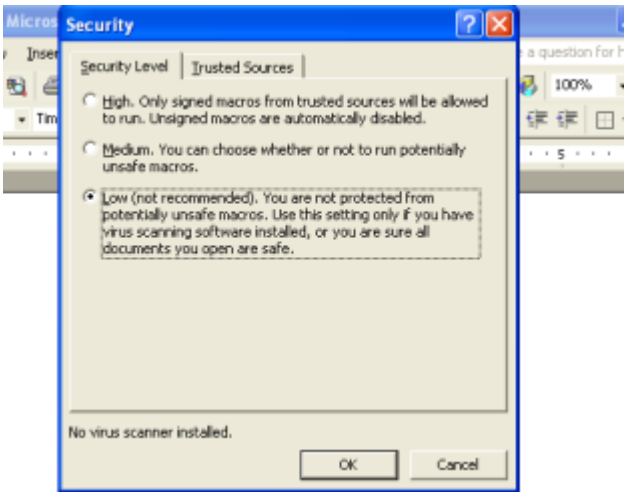
Schritt	Details
Schritt 52: Um Microsoft Word-, Excel- und PowerPoint-Dateien zu analysieren, installieren Sie Microsoft Office 2003 auf dem virtuellen Computer.	
Schritt 53: Senken Sie die Sicherheitsstufe, um Makros für Office-Anwendungen auszuführen.	• Öffnen Sie Microsoft Word 2003, und wählen Sie **Extras** | **Makro** | **Sicherheit** und dann **Niedrig**, und klicken Sie auf **OK**.  • Setzen Sie genauso die Makrosicherheit für Microsoft Excel und PowerPoint herab.

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

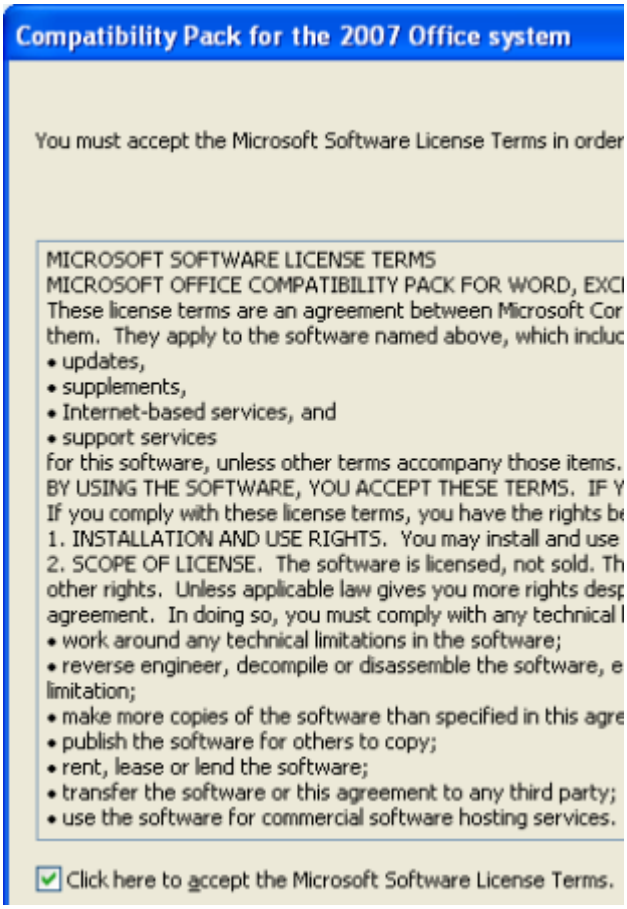
Schritt	Details
Schritt 54: Sie benötigen das Compatibility Pack, um Microsoft Office-Dateien öffnen zu können, die mit einer neueren Version von Microsoft Office erstellt wurden. Beispiel: Zum Öffnen einer DOCX-Datei mit Office 2003 muss das entsprechende Compatibility Pack installiert sein. Rufen Sie http://www.microsoft.com/en-us/download/details.aspx?id=3 auf, und laden Sie das erforderliche Microsoft Office Compatibility Pack für Word-, Excel- und PowerPoint-Dateiformate herunter. Installieren Sie es anschließend auf dem virtuellen Computer.	
Schritt 55: Aktivieren Sie im Dialogfeld **Compatibility Pack für 2007 Office System** die Option **Klicken Sie hier, um den Microsoft-Software-Lizenzbedingungen zuzustimmen**, und klicken Sie auf **OK**.	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

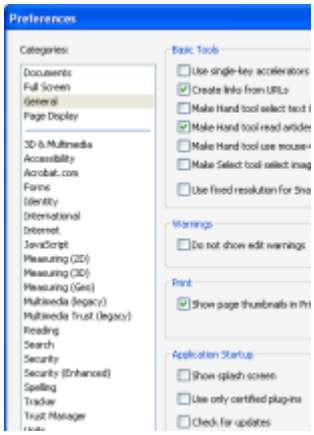
Schritt	Details
Schritt 56: Um PDF-Dateien zu analysieren, laden Sie Adobe Reader auf den nativen Host herunter, und kopieren Sie ihn auf die VM. In diesem Beispiel wird Adobe Reader 9.0 verwendet.	1 Installieren Sie Adobe Reader 9.0 auf der VM. 2 Öffnen Sie Adobe Reader, und klicken Sie auf **Akzeptieren**.  3 Wählen Sie in Adobe Reader **Bearbeiten** | **Voreinstellungen** | **Allgemein** , und deaktivieren Sie **Nach Updates suchen**. 
Schritt 57: Laden Sie die folgenden Programme auf den nativen Host herunter, und installieren Sie sie auf der VM.	1 Laden Sie Microsoft Visual C++ 2005 Redistributable Package (x86) von der Seite http://www.microsoft.com/en-us/download/details.aspx?id=3387 herunter,und installieren Sie das Programm. 2 Laden Sie Microsoft Visual C++ 2008 Redistributable Package (x86) von der Seite http://www.microsoft.com/en-us/download/details.aspx?id=5582 herunter,und installieren Sie das Programm. 3 Laden Sie Microsoft Visual C++ 2010 Redistributable Package (x86) von der Seite http://www.microsoft.com/en-us/download/details.aspx?id=5555 herunter,und installieren Sie das Programm. 4 Laden Sie Microsoft .NET Framework 2.0 Service Pack 2 (x86-Version) von der Seite http://www.microsoft.com/en-us/download/details.aspx?id=1639 herunter,und installieren Sie das Programm.

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

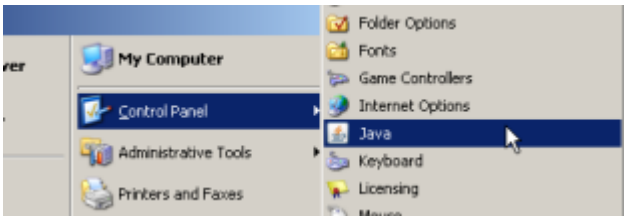
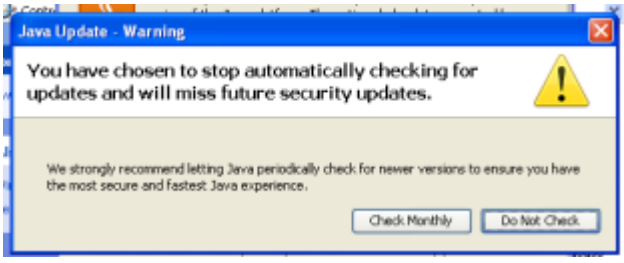
Schritt	Details
Schritt 58: Laden Sie zum Analysieren von JAR-Dateien Java Runtime Environment herunter, und installieren Sie die Anwendung. In diesem Beispiel wird Java 7 Update 25 verwendet.	
Schritt 59: Öffnen Sie Java in der Systemsteuerung.	
Schritt 60: Deaktivieren Sie auf der Registerkarte **Update** die Option **Automatisch nach Updates suchen**.	
Schritt 61: Wählen Sie im Dialogfeld "Java-Update – Warnung" die Option **Nicht überprüfen**, und klicken Sie dann in der Java-Systemsteuerung auf **OK**.	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

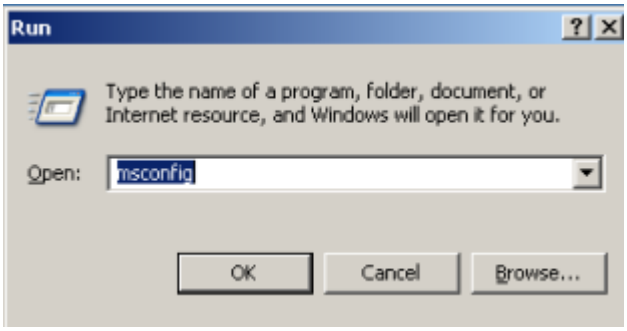
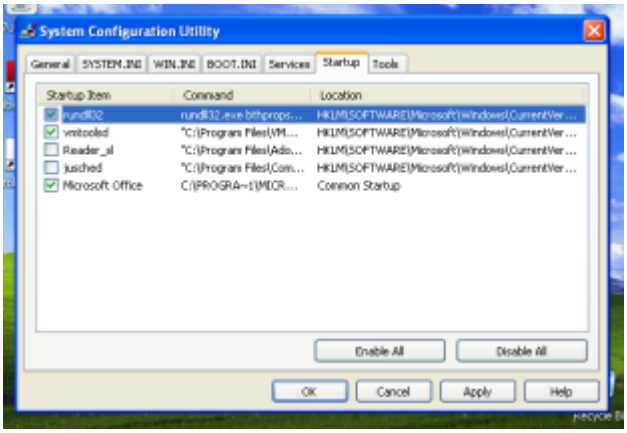
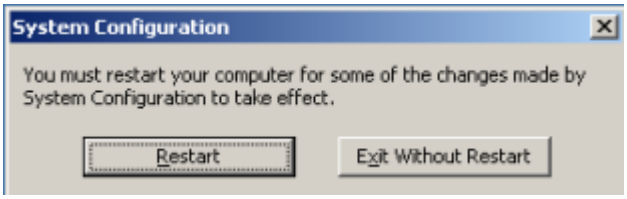
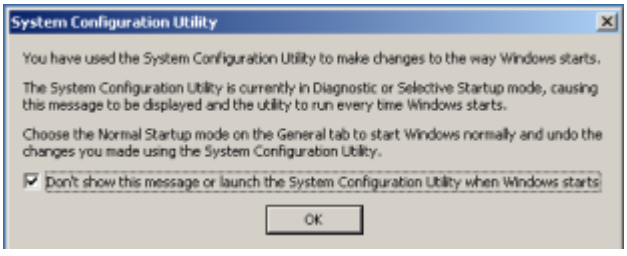
Schritt	Details
Schritt 62: Geben Sie im Windows-Dialogfeld "Ausführen" `msconfig` ein.	
Schritt 63: Navigieren Sie im Systemkonfigurationsprogramm zur Registerkarte **Start**.	 Deaktivieren Sie *reader_sl* und *jusched*, und klicken Sie dann auf **OK**. Der Eintrag "reader_sl" wird nur angezeigt, wenn Adobe Reader installiert ist.
Schritt 64: Klicken Sie in der **Systemkonfiguration** auf **Neu starten**.	
Schritt 65: Aktivieren Sie im Dialogfeld **Systemkonfigurationsprogramm** das Kontrollkästchen **Meldung nicht mehr anzeigen und dieses Programm beim Windows-Start nicht mehr starten**, und klicken Sie auf **OK**.	

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

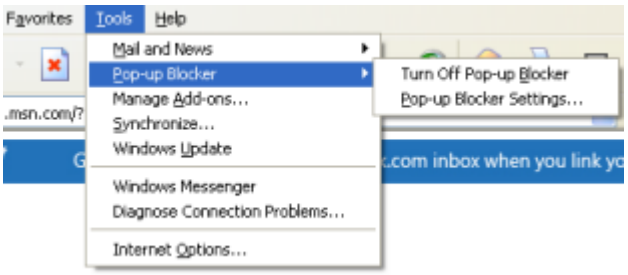
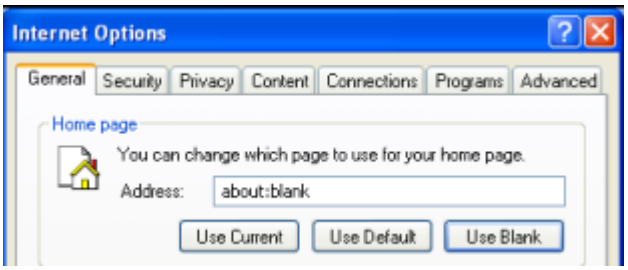
Schritt	Details
Schritt 66: Öffnen Sie den Standard-Browser, und richten Sie ihn für Malware-Analysen ein. In diesem Beispiel wird Internet Explorer verwendet.	1 Stellen Sie sicher, dass der Popupblocker ausgeschaltet ist. Wählen Sie in Internet Explorer **Extras** | **Popupblocker** | **Popupblocker ausschalten.**  2 Wählen Sie **Extras** | **Internetoptionen** , und wählen Sie abhängig von der Version von Internet Explorer unter **Startseite** entweder **Leere Seite** oder **Neue Registerkarte** aus.  3 Wechseln Sie zur Registerkarte **Erweitert,** und suchen Sie **Sicherheit.** 4 Wählen Sie **Ausführung aktiver Inhalte in Dateien auf dem lokalen Computer zulassen** aus.

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

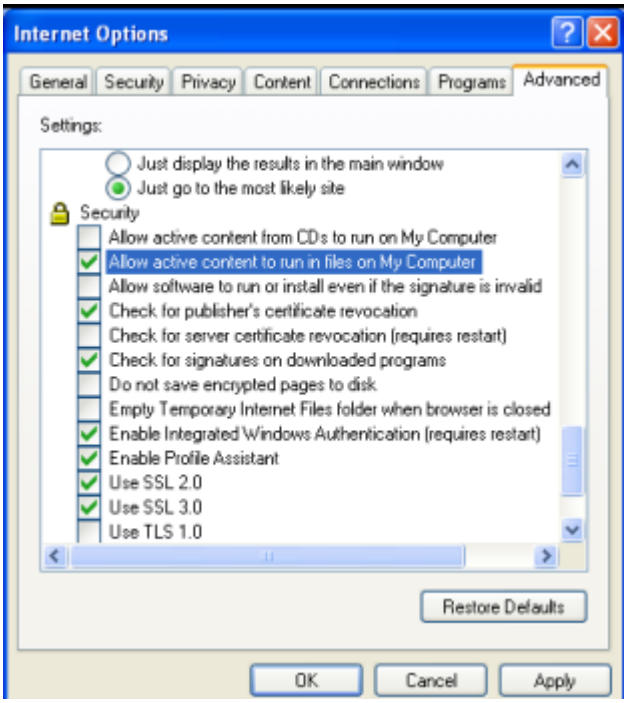
Schritt	Details
	 **5** Klicken Sie auf **OK**.

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

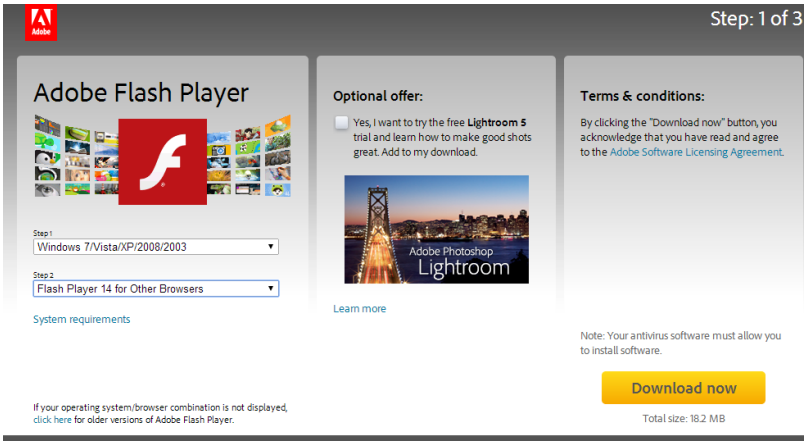
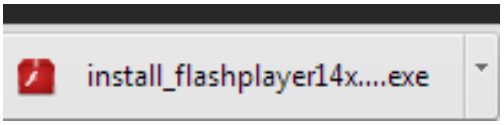
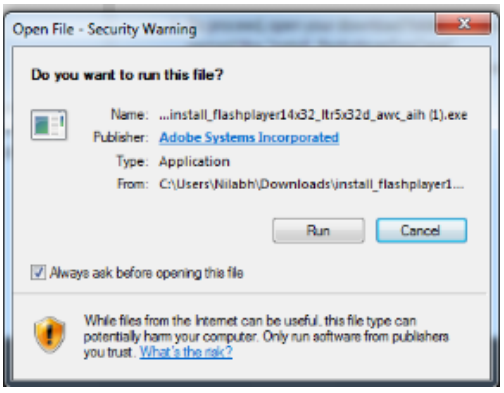
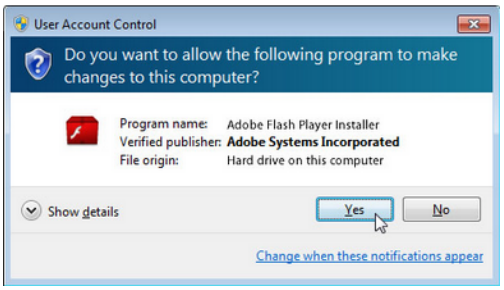
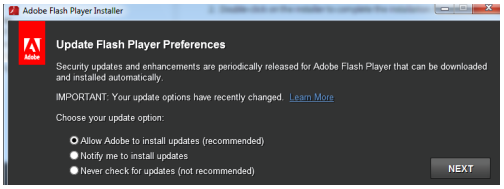
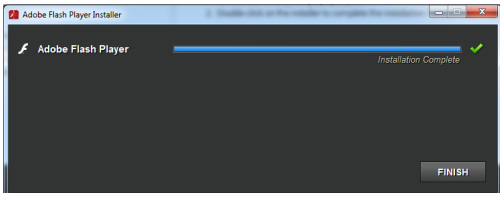
Schritt	Details
Schritt 67: Um eine Flash-Datei (SWF) dynamisch zu analysieren, laden Sie die erforderliche Version von Adobe Flash herunter. In diesem Beispiel wird Flash Player 14 verwendet.	1 Rufen Sie http://get.adobe.com/de/flashplayer/otherversions/ auf. 2 Wählen Sie gemäß Ihren Anforderungen ein Betriebssystem und eine Flash Player-Version in den Dropdown-Menüs **Schritt 1** und **Schritt 2** aus (siehe unten). 3 Klicken Sie auf **Jetzt herunterladen**.  4 Doppelklicken Sie in der unteren Ecke Ihres Bildschirms auf die Installationsdatei für Adobe Flash Player **(install_flashplayer xxx.exe)**.  5 Klicken Sie im Dialogfeld **Sicherheitswarnung** auf **Ausführen**.  6 Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.

Tabelle 5-3 Erstellen einer VMDK-Datei aus einem ISO-Image von Windows 2003 Server SP1 oder SP2 *(Fortsetzung)*

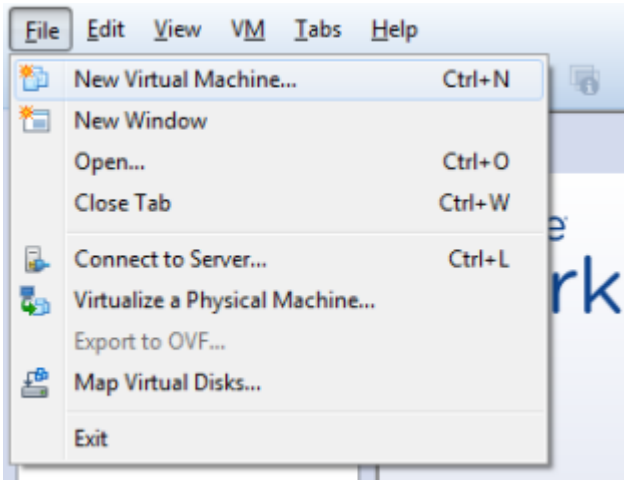
Schritt	Details
	 **7** Wählen Sie Ihre Aktualisierungsoption, und klicken Sie auf **WEITER**.  **8** Klicken Sie auf **FERTIGSTELLEN**, um die Adobe Flash Player-Installation abzuschließen. 
Schritt 68: Fahren Sie das virtualMachineImage herunter, indem Sie folgende Optionen auswählen: **Start** | **Herunterfahren** | **Herunterfahren** | **OK**.	
Schritt 69: Navigieren Sie zu dem Speicherort, den Sie in Schritt 7 angegeben haben, um die VMDK-Datei mit dem Namen `virtualMachineImage-flat.vmdk` aufzurufen.	

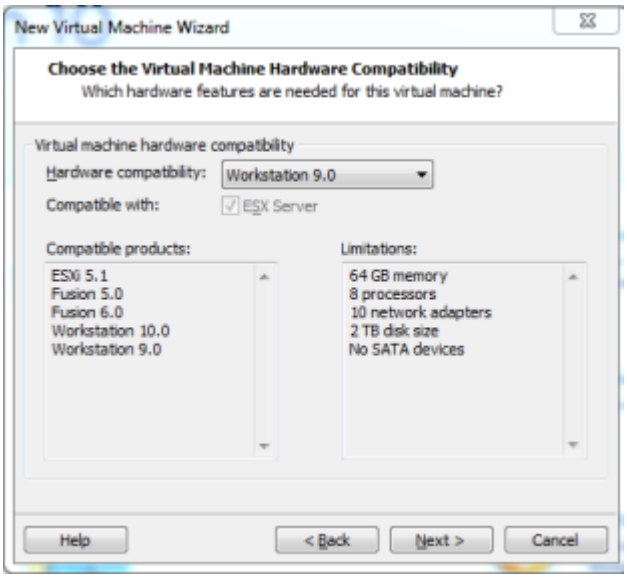
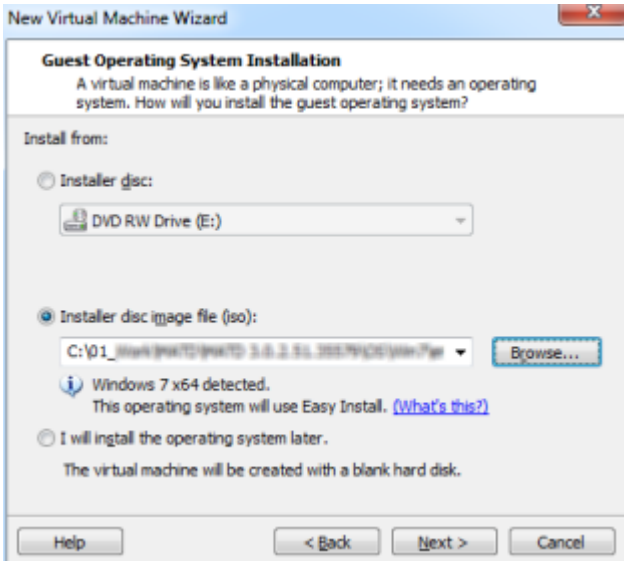
Erstellen einer VMDK-Datei für Windows 7

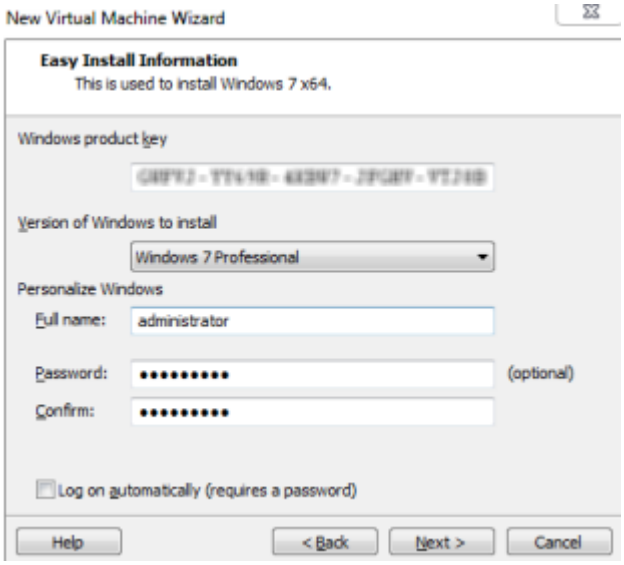
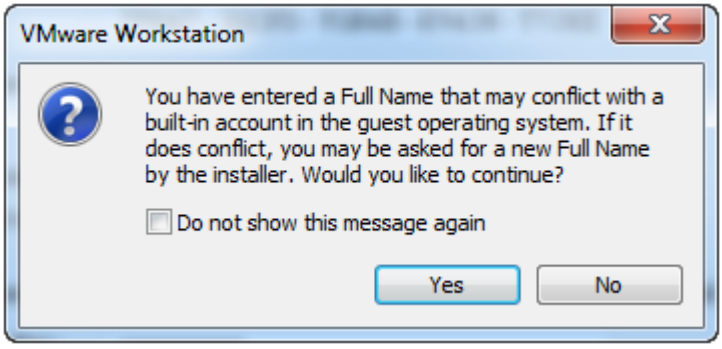
Bevor Sie beginnen

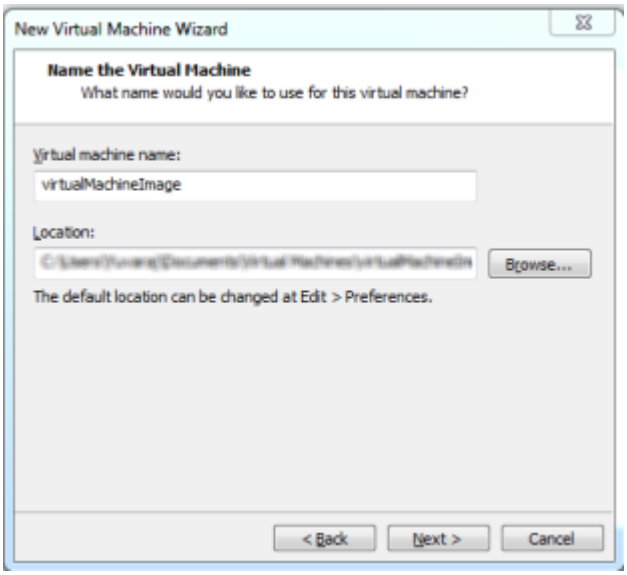
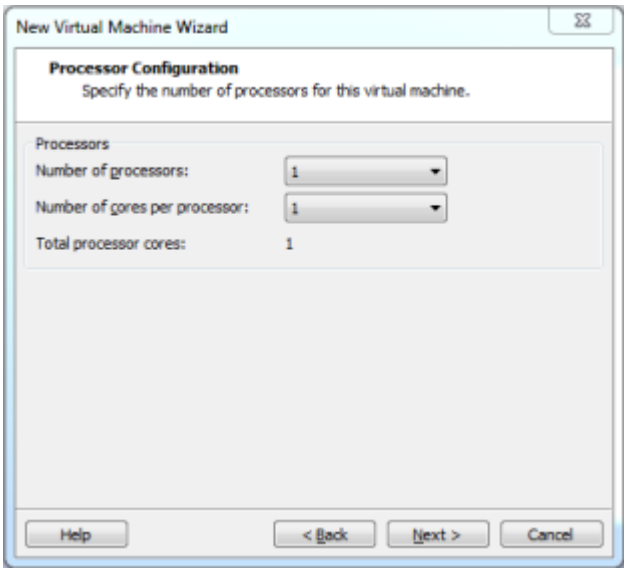
- Laden Sie VMware Workstation 9.0 oder höher von der Seite http://www.vmware.com/products/workstation/workstation-evaluation herunter, und installieren Sie das Programm.
- Stellen Sie sicher, dass Sie über ein ISO-Image von Windows 7 SP1 32 oder 64 Bit verfügen, für das Sie die VMDK-Datei erstellen müssen. Windows Enterprise Edition und Windows Professional werden unterstützt.
- Stellen Sie sicher, dass Sie über den Lizenzschlüssel für das Betriebssystem verfügen.

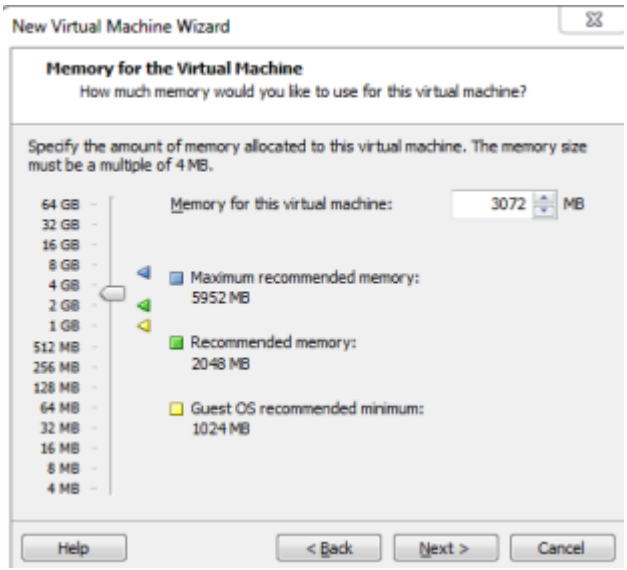
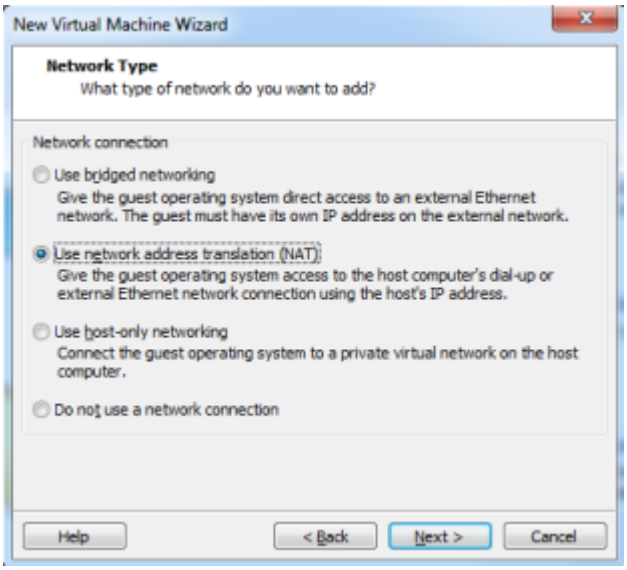
Gehen Sie wie nachfolgend beschrieben vor, um VMDK-Dateien von einem ISO-Image von Windows 7 SP1 32 oder 64 Bit zu erstellen.

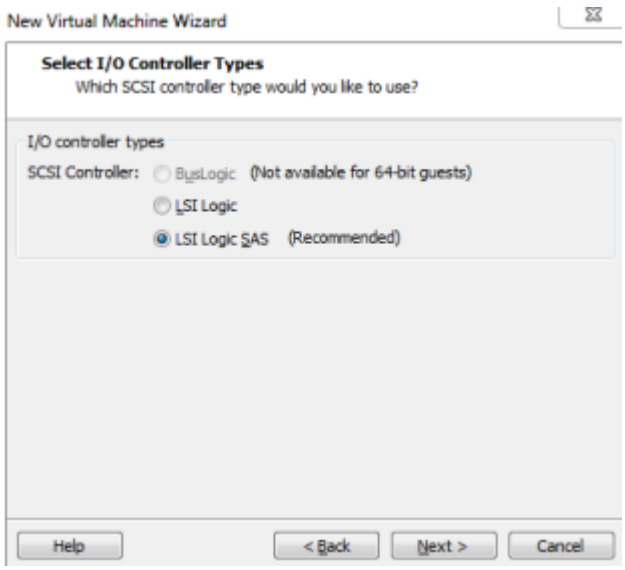
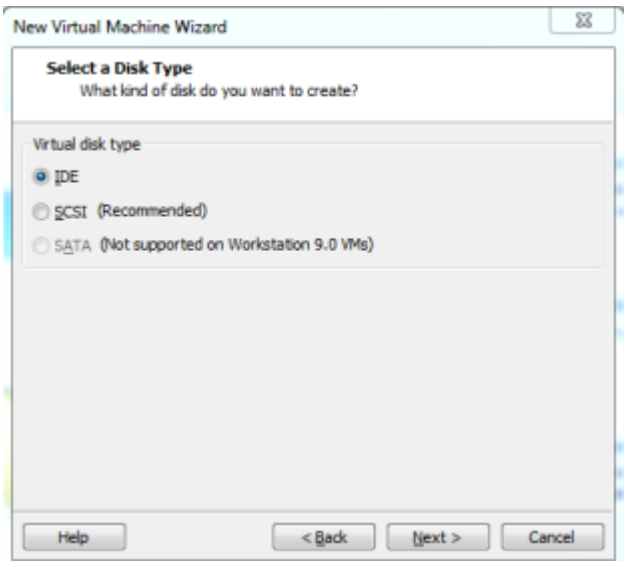
Schritt	Details
Schritt 1: Starten Sie VMware Workstation.	In diesem Beispiel wird VMware Workstation 10 verwendet.
Schritt 2: Wählen Sie auf der VMware Workstation-Seite **Datei | New Virtual Machine (Neuer virtueller Computer)**.	
Schritt 3: Wählen Sie im Fenster **New Virtual Machine Wizard** (Assistent für neue virtuelle Computer) die Option **Custom (Advanced)** (Benutzerdefiniert (erweitert)), und klicken Sie auf **Next** (Weiter).	

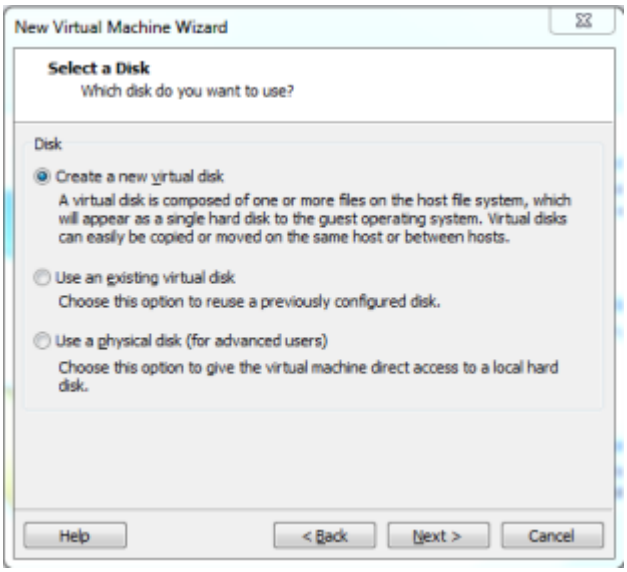
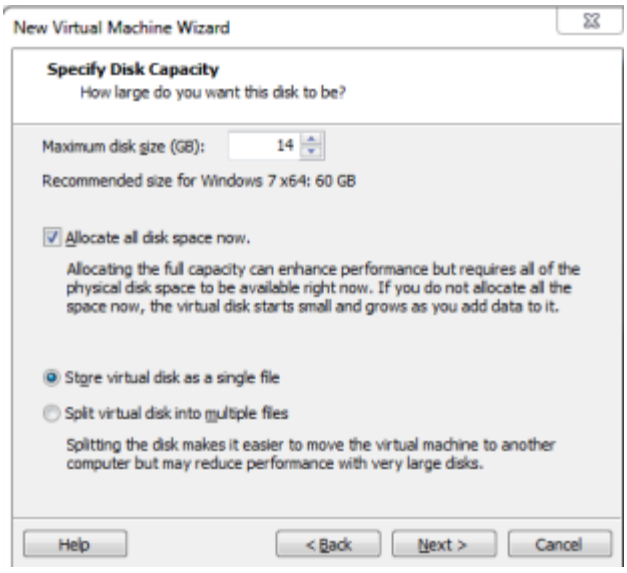
Schritt	Details
Schritt 4: Wählen Sie im Fenster **Choose the Virtual Machine Hardware Compatibility** (Wählen der Hardwarekompatibilität des virtuellen Computers) **Workstation 9.0** aus der Dropdown-Liste **Hardware compatibility** (Hardwarekompatibilität) aus. Akzeptieren Sie bei den anderen Feldern die Standardwerte, und klicken Sie auf **Next** (Weiter).	
Schritt 5: Wählen Sie im Fenster **Guest Operating System Installation** (Installation eines Gast-Betriebssystems) entweder **Installer disc** (Installationsdatenträger) oder **Installer disc image file (iso)** (Image-Datei des Installationsdatenträgers), navigieren Sie zum ISO-Image, wählen Sie es aus, und klicken Sie anschließend auf **Next** (Weiter).	

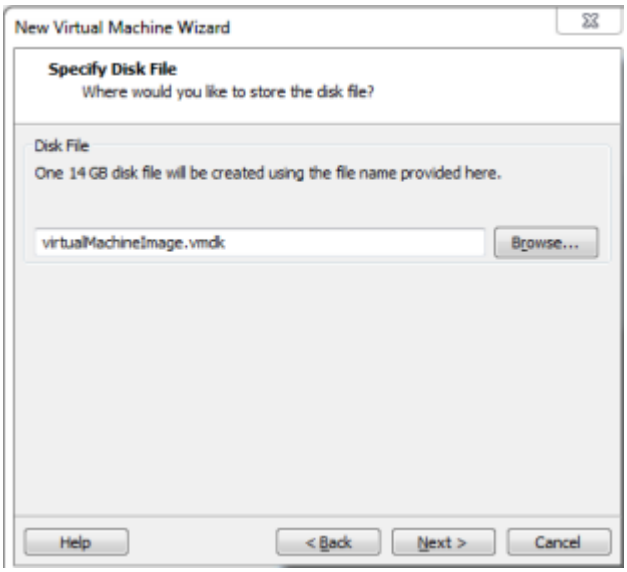
Schritt	Details
Schritt 6: Geben Sie die Informationen im Fenster **Easy Install Information** (Informationen zur einfachen Installation) ein, und klicken Sie auf **Next** (Weiter).	• **Windows product key** (Windows-Produktschlüssel) – Geben Sie den Lizenzschlüssel des Windows-Betriebssystems ein, für das Sie die VMDK-Datei erstellen. • **Full name** (Vollständiger Name) – Geben Sie `administrator` als **Full name** ein. • **Password** (Kennwort) – Geben Sie `cr@cker42` als Kennwort ein. Dies ist das Kennwort, das McAfee Advanced Threat Defense für die Anmeldung bei der VM verwendet. • **Confirm** (Bestätigen) – Geben Sie `cr@cker42` zur Bestätigung erneut ein. • **Log on automatically (requires a password)** (Automatisch anmelden; Kennwort erforderlich) – Deaktivieren Sie dieses Kontrollkästchen. 
Schritt 7: Klicken Sie im Popupfenster **VMware Workstation** auf **Yes** (Ja).	

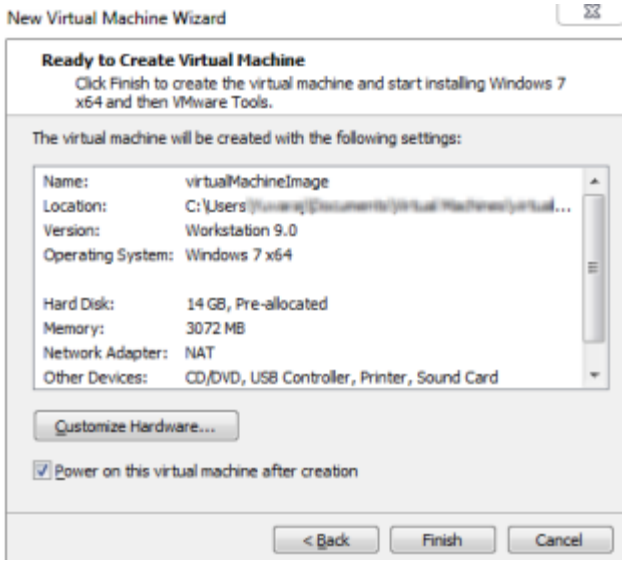
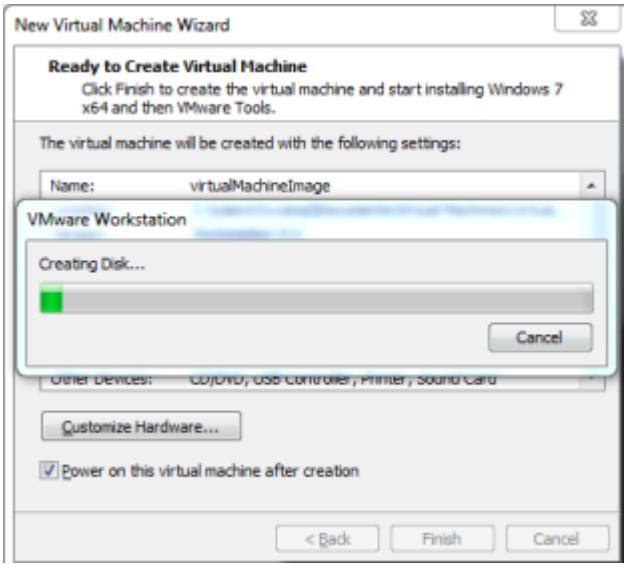
Schritt	Details
Schritt 8: Geben Sie die Informationen im Fenster **Name the Virtual Machine** (Benennen des virtuellen Computers) ein, und klicken Sie anschließend auf **Next** (Weiter).	• **Virtual Machine name** (Name des virtuellen Computers) – Geben Sie `virtualMachineImage` als Namen ein. • **Location** (Speicherort) – Navigieren Sie zu dem Ordner, in dem die VDMK-Datei erstellt werden soll, und wählen Sie ihn aus. 
Schritt 9: Übernehmen Sie im Fenster **Processor Configuration** (Prozessorkonfiguration) die Standardwerte, und klicken Sie auf **Next** (Weiter).	

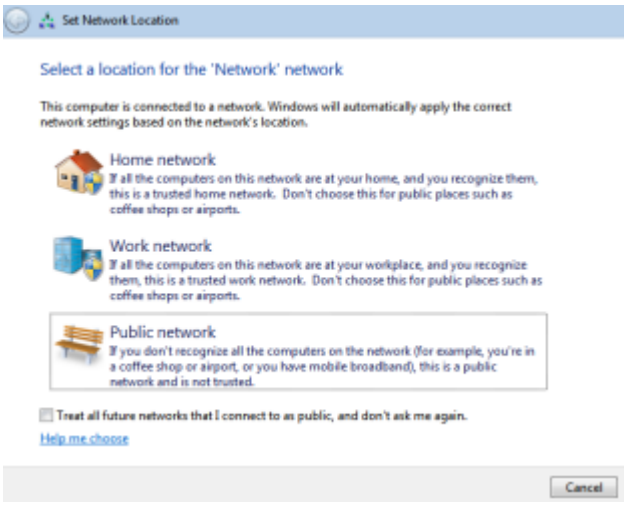
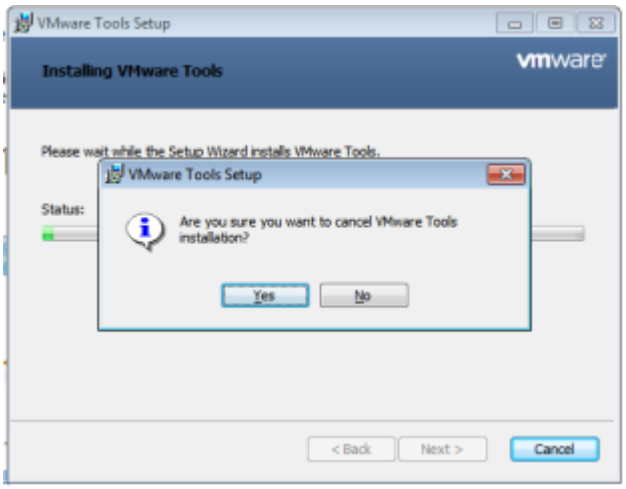
Schritt	Details
Schritt 10: Legen Sie im Fenster **Memory for the Virtual Machine** (Speicher für den virtuellen Computer) 3.072 MB als Speicher fest.	
Schritt 11: Übernehmen Sie im Fenster **Network Type** (Netzwerktyp) die Standardauswahl.	

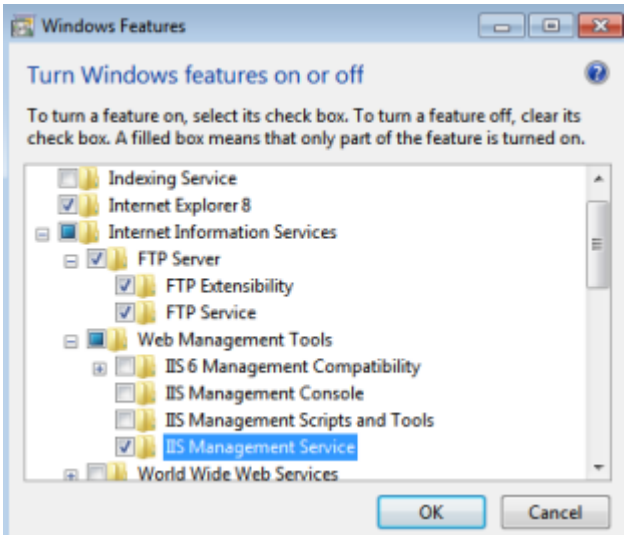
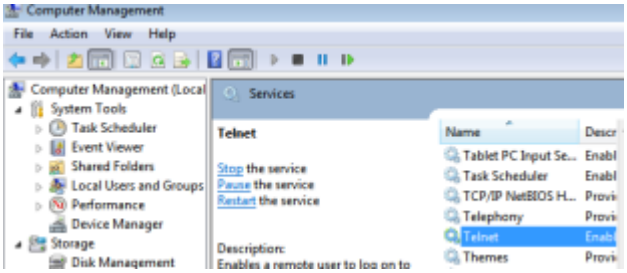
Schritt	Details
Schritt 12: Übernehmen Sie unter **Select I/O Controller Types** (Auswählen der I/O-Controller-Typen) die Standardauswahl.	
Schritt 13: Wählen Sie auf der Seite **Auswählen eines Datenträgertyps** die Option **IDE**, und klicken Sie auf **Next** (Weiter). SCSI-Datenträger sind mit McAfee Advanced Threat Defense nicht kompatibel.	

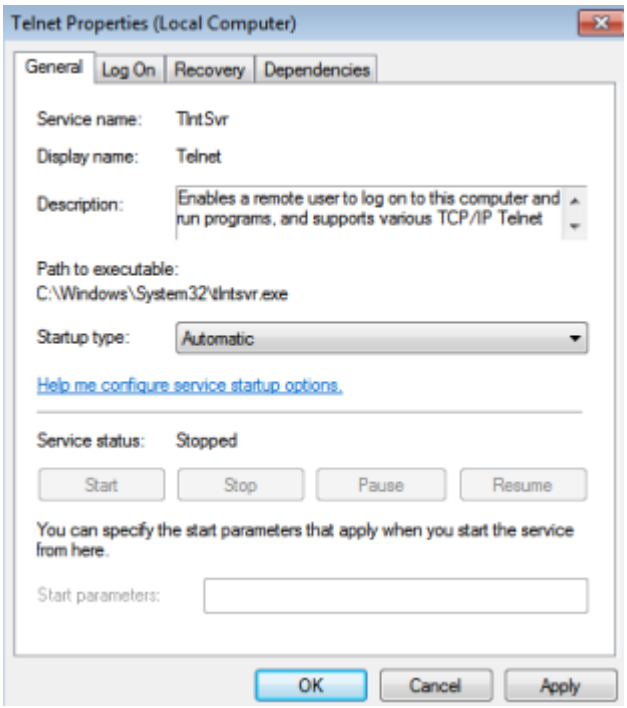
Schritt	Details
Schritt 14: Wählen Sie im Fenster **Auswählen eines Datenträgers** die Option **Create a new virtual disk** (Neuen virtuellen Datenträger erstellen), und klicken Sie auf **Next** (Weiter).	
Schritt 15: Geben Sie die Details im Fenster **Angeben der Speicherkapazität** an, und klicken Sie auf **Next** (Weiter).	• **Maximum disk size (GB)** (Maximale Datenträgergröße in GB) – Geben Sie für Windows 7 (64 Bit) 14 GB ein. Geben Sie für Windows 7 (32 Bit) 12 GB ein. • Wählen Sie **Allocate all disk space now** (Sämtlichen Speicherplatz jetzt zuweisen). • Wählen Sie **Store virtual disk as a single file** (Virtuellen Datenträger als einzelne Datei speichern). 

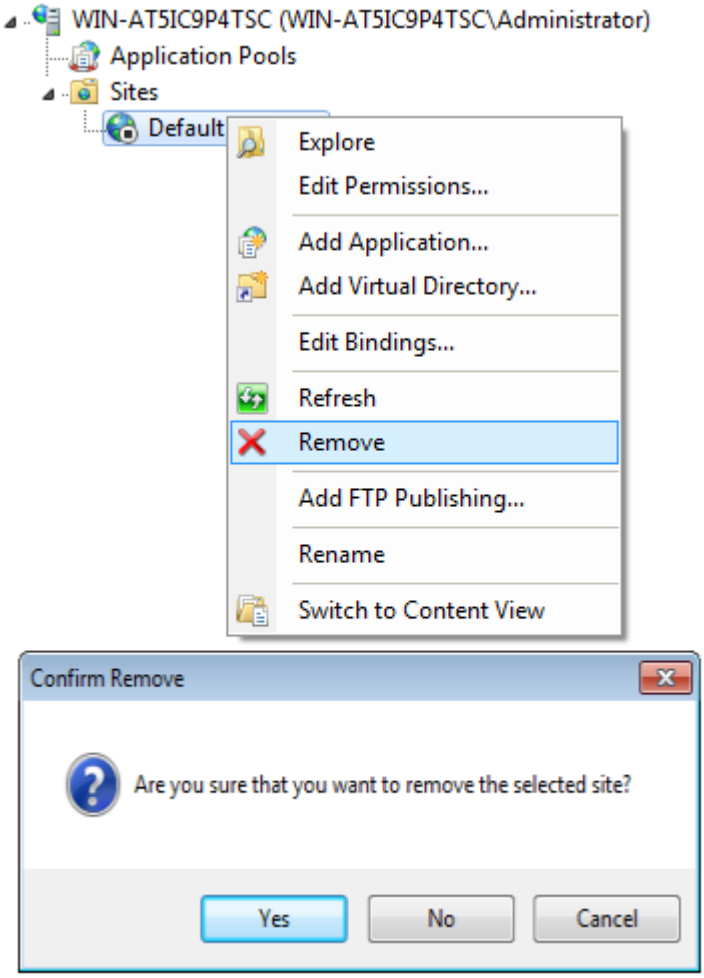
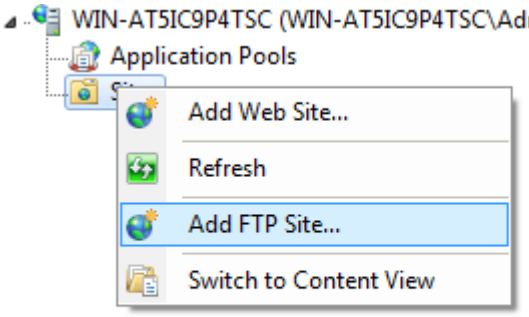
Schritt	Details
Schritt 16: Vergewissern Sie sich, dass im Fenster **Specify Disk file** (Datenträgerdatei angeben) standardmäßig "virtualMachineImage.vmdk" angezeigt wird, und klicken Sie auf **Next** (Weiter). Wenn Sie unter **Virtual Machine name** (Name des virtuellen Computers) einen anderen Namen angegeben haben, wird dieser hier angezeigt.	

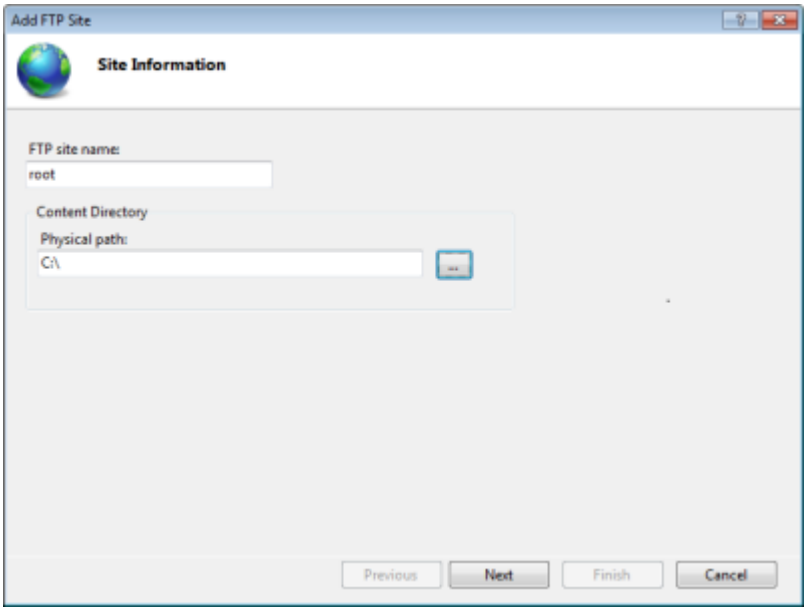
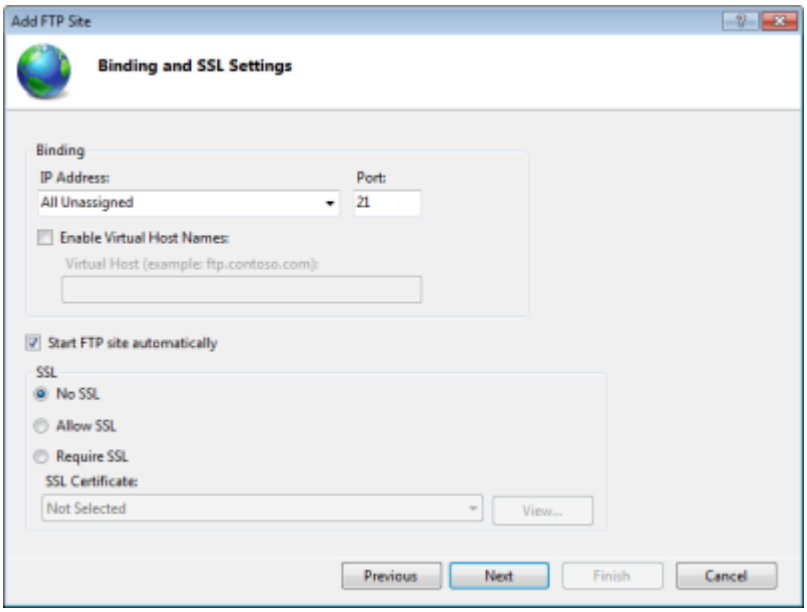
Schritt	Details
Schritt 17: Führen Sie folgende Schritte im Fenster **Ready to Create Virtual Machine** (Bereit zur Erstellung des virtuellen Computers) aus.	• **Power on this virtual machine after creation** (Diesen virtuellen Computer nach der Erstellung einschalten) – Wählen Sie diese Option. • Klicken Sie auf **Finish** (Fertig stellen). Dieser Schritt kann etwa 30 Minuten in Anspruch nehmen.  
Schritt 18: Wenn das Popupfenster **Removable Devices** (Wechselgeräte) angezeigt wird, wählen Sie **Do not show this hint again** (Diesen Hinweis nicht mehr anzeigen), und klicken Sie auf **OK**.	Die Installation von Windows beginnt. Dies kann etwa 15 Minuten dauern.

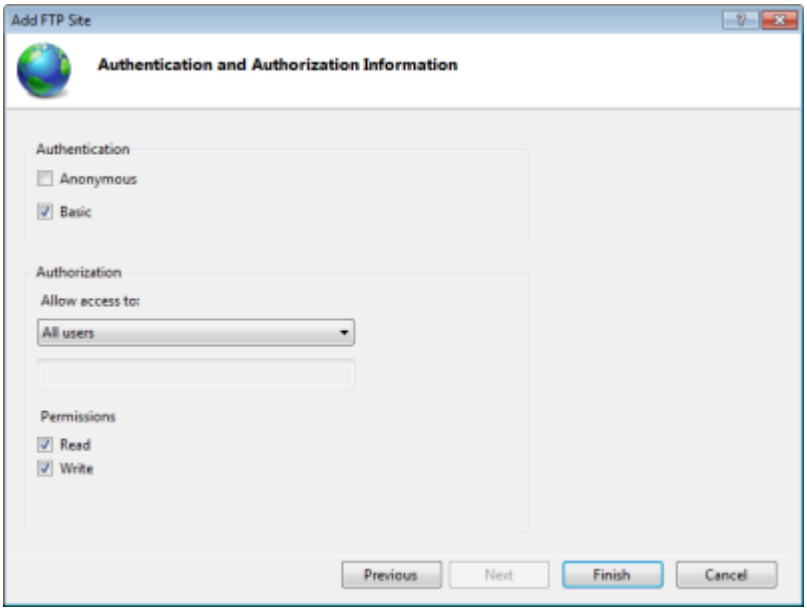
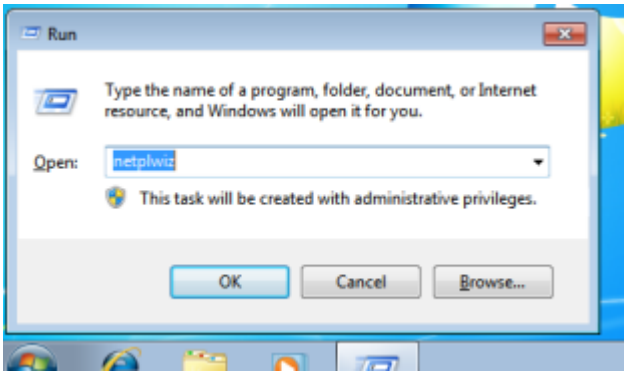
Schritt	Details
Schritt 19: Wenn das Fenster **Set Network Location** (Netzwerkstandort festlegen) angezeigt wird, wählen Sie **Public Network** (Öffentliches Netzwerk) und **Close** (Schließen).	
Schritt 20: Halten Sie die Installation von VMware Tools an. Die VMware Tools sind mit McAfee Advanced Threat Defense nicht kompatibel. Wenn Sie die Installation von VMware Tools nicht angehalten haben, können Sie dennoch mit der VMDK-Dateierstellung fortfahren. Das Programm muss aber deinstalliert sein, sobald die VMDK-Datei bereit ist.	
Schritt 23: Deaktivieren Sie auf der VM die Windows-Firewall.	1 Wählen Sie **Start** | **Systemsteuerung** | **System und Sicherheit** | **Windows-Firewall** | **Windows-Firewall ein- oder ausschalten** 2 Wählen Sie **Windows-Firewall deaktivieren (nicht empfohlen)** für sowohl **Standorteinstellungen für das Heim- oder Arbeitsplatznetzwerk (privat)** als auch **Standorteinstellungen für das öffentliche Netzwerk**, und klicken Sie anschließend auf **OK**.

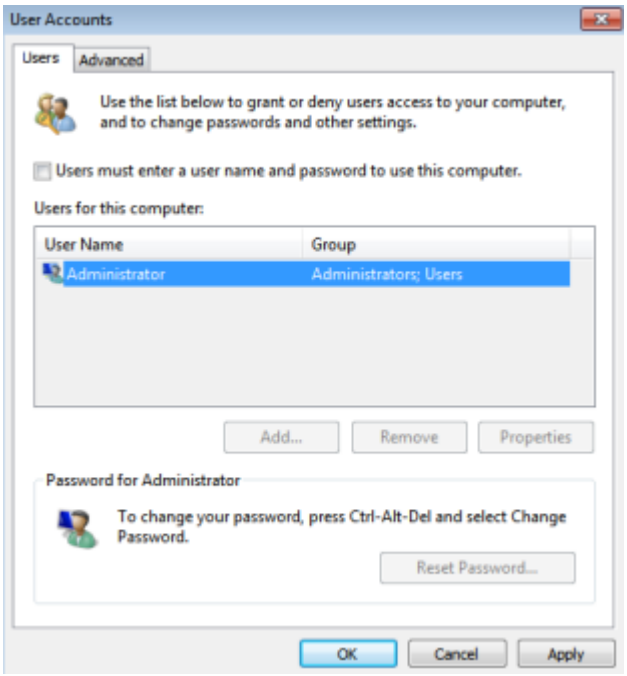
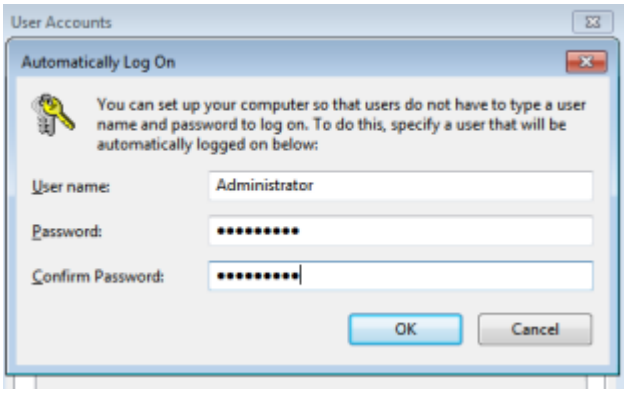
Schritt	Details
Schritt 24: Wählen Sie **Start** | **Systemsteuerung** | **Programme** | **Programme und Funktionen** | **Windows-Funktionen ein- oder ausschalten** , und führen Sie folgende Schritte aus.	1 Wählen Sie **Internetinformationsdienste** | **FTP-Server** und **FTP-Erweiterbarkeit**. 2 Wählen Sie **Internetinformationsdienste** | **Webverwaltungstools** und **IIS-Webverwaltungsdienst**. 3 Wählen Sie **Telnet-Server**, und klicken Sie auf "OK". Dieser Vorgang kann etwa 5 Minuten in Anspruch nehmen. 
Schritt 25: Klicken Sie auf **Start** und dann mit der rechten Maustaste auf **Computer**. Wählen Sie dann **Verwalten** | **Dienste und Anwendungen** | **Dienste**. Doppelklicken Sie anschließend auf **Telnet**.	

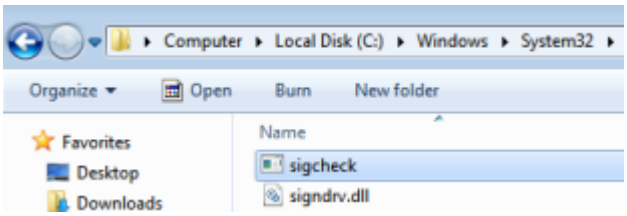
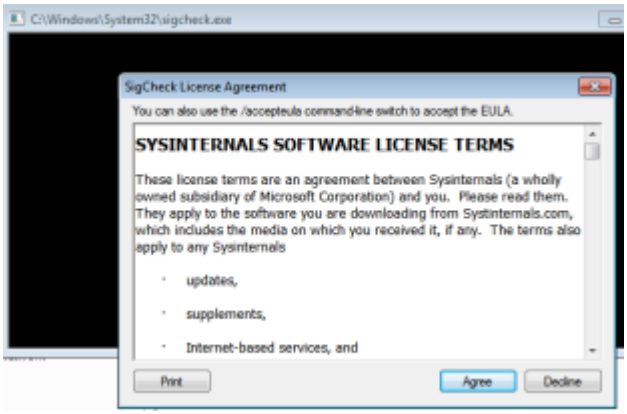
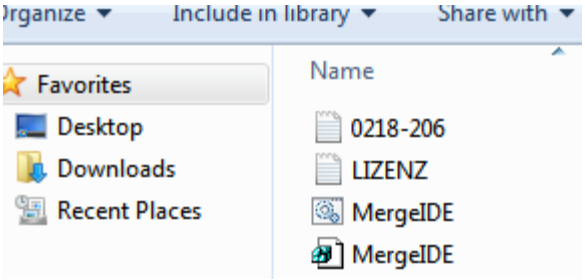
Schritt	Details
Schritt 26: Wählen Sie im Dialogfeld "Eigenschaften von Telnet (Lokaler Computer)" aus der Liste **Starttyp** die Option **Automatisch** aus. Wählen Sie dann **Übernehmen** | **Start** | **OK**.	

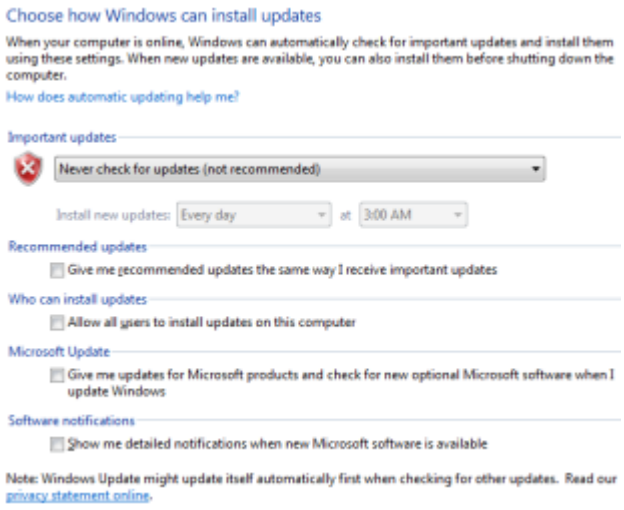
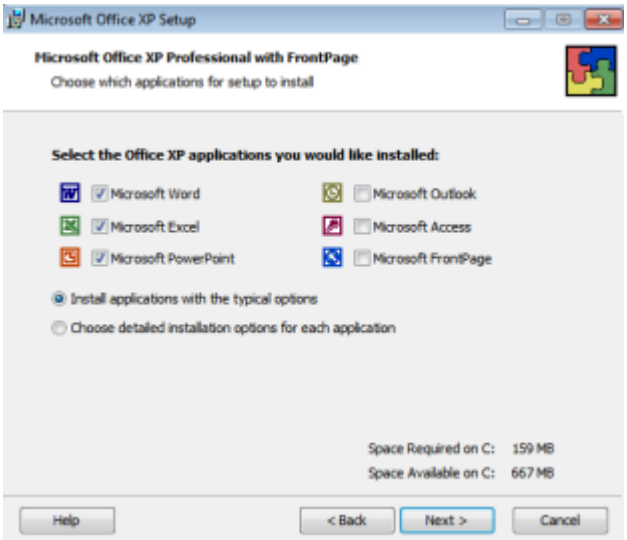
Schritt	Details
Schritt 27: Aktivieren Sie FTP auf der VM. Wählen Sie im virtualMachineImage die Optionen **Start** | **Systemsteuerung** | **System und Sicherheit** | **Verwaltung**. Doppelklicken Sie auf **Internetinformationsdienste (IIS)**, erweitern Sie die Baumstruktur unter **Hostname**, und führen Sie folgende Schritte aus:	1 Wählen Sie **Sites** und klicken Sie mit der rechten Maustaste auf **Standardwebsite** und anschließend auf "Entfernen". Bestätigen Sie den Vorgang, indem Sie auf **Ja** klicken.  2 Klicken Sie mit der rechten Maustaste auf **Sites**, und wählen Sie **FTP-Site hinzufügen**. Führen Sie dann folgende Schritte aus.  a Geben Sie unter **FTP-Sitename** `root` ein.

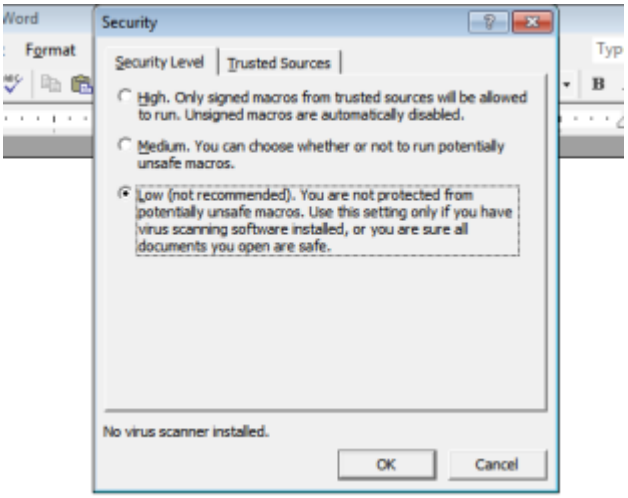
Schritt	Details
	b **Physischer Pfad: C:\.** **c** Klicken Sie auf **Weiter.**  **3** Wählen Sie unter **Bindungen und SSL-Einstellungen** die Option **Kein SSL.** Akzeptieren Sie bei allen anderen Feldern die Standardwerte, und klicken Sie auf **Weiter.**  **Abbildung 5-1 Bindungs- und SSL-Einstellungen** **4** Führen Sie unter **Authentifizierungs- und Autorisierungsinformationen** folgende Schritte aus. **a** Wählen Sie **Standard.** **b** Unter **Zugriff zulassen für** wählen Sie **Alle Benutzer.**

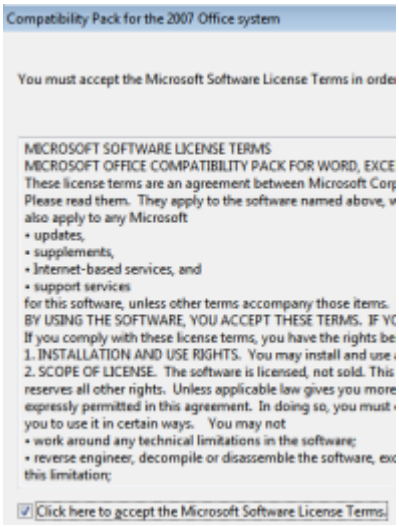
Schritt	Details
	c Wählen Sie unter **Berechtigungen** sowohl **Lesen** als auch **Schreiben**, und klicken Sie anschließend auf **Fertig stellen**. d Schließen Sie das Fenster **Internetinformationsdienste-Manager**. 
Schritt 28: Wählen Sie **Start** | **Ausführen**, geben Sie `netplwiz` ein, und klicken Sie auf **OK**.	

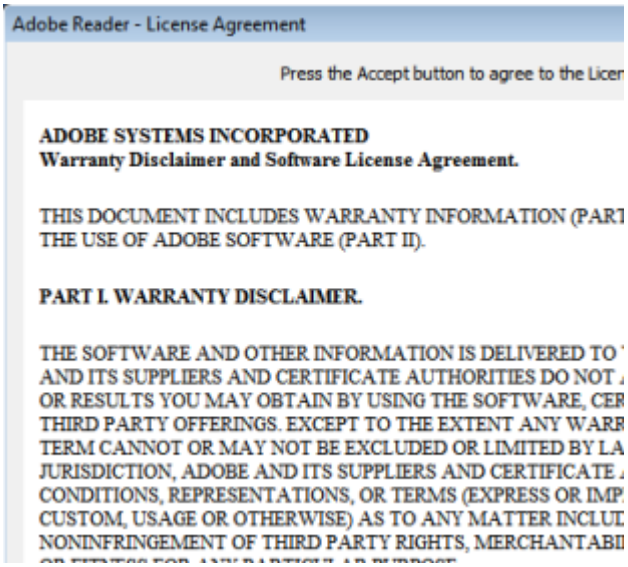
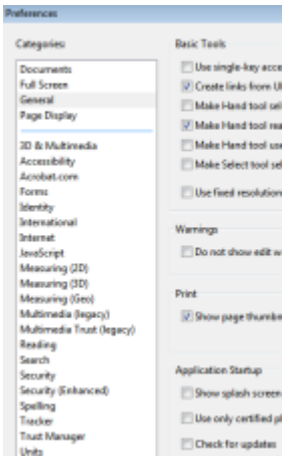
Schritt	Details
Schritt 29: Deaktivieren Sie im Fenster **Benutzerkonten** die Option **Benutzer müssen Benutzernamen und Kennwort eingeben**, und klicken Sie auf **Übernehmen**.	
Schritt 30: Führen Sie im Popupfenster **Automatische Anmeldung** die folgenden Schritte aus, und klicken Sie dann auf **OK**.	• **Benutzername** – Geben Sie `Administrator` ein. • **Kennwort** – Geben Sie `cr@cker42` ein. • **Kennwort bestätigen** – Geben Sie `cr@cker42` erneut ein. 
Schritt 31: Laden Sie Sigcheck von der Seite http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx auf Ihren Computer (den nativen Host) herunter.	Auf der von Ihnen erstellten VM ist die Windows-Firewall deaktiviert. Außerdem ist kein Virenschutz installiert. Daher wird empfohlen, die Programme und Komponenten zuerst auf den nativen Host herunterzuladen und dann auf die VM in VMware Workstation zu kopieren.
Schritt 32: Extrahieren Sie "sigcheck.zip" an folgendem Speicherort: `C:\WINDOWS\system32`.	

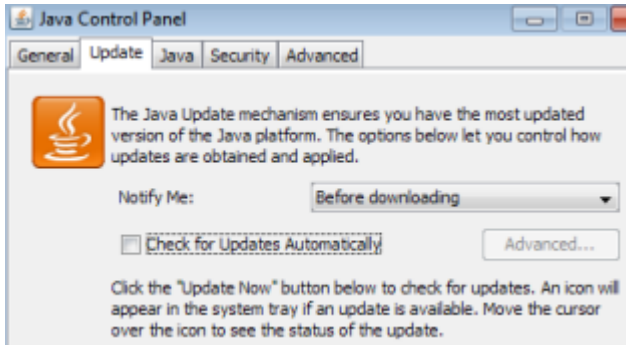
Schritt	Details
Schritt 33: Navigieren Sie in Windows Explorer zu C:\WINDOWS\system32, und doppelklicken Sie auf **sigcheck.exe**.	
Schritt 34: Klicken Sie im **Sigcheck License Agreement** (Sigcheck-Lizenzvertrag) auf **Agree** (Ich stimme zu). Nach dem Klicken auf **Agree** (Ich stimme zu) wird keine Bestätigungsmeldung angezeigt.	
Schritt 35: Laden Sie die ZIP-Datei "MergeIDE.zip" von der Seite https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip auf den nativen Computer herunter, und kopieren Sie sie auf die VM.	
Schritt 36: Extrahieren Sie MergeIDE.zip, und führen Sie die MergeIDE-Batchdatei auf der VM aus.	• Klicken Sie in der Warnmeldung auf **Ausführen**, wenn Sie dazu aufgefordert werden. • Schließen Sie Windows Explorer.

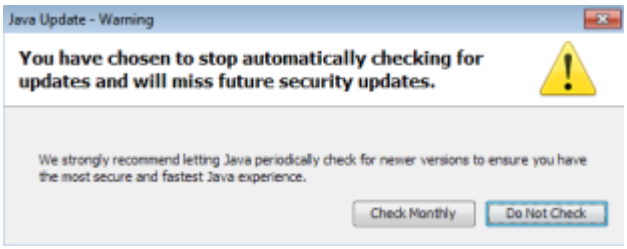
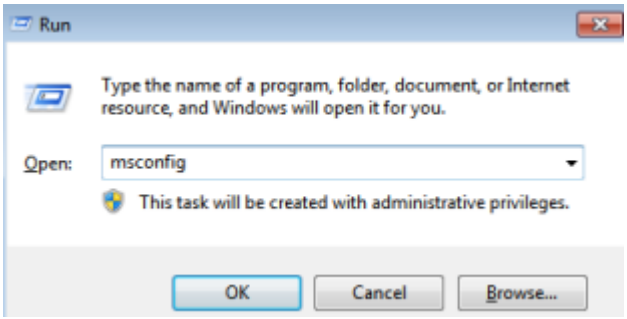
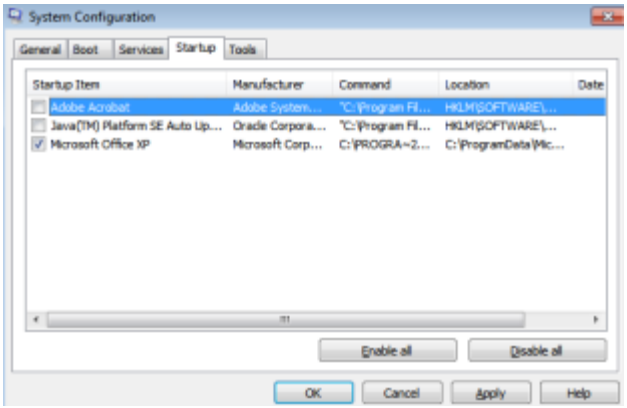
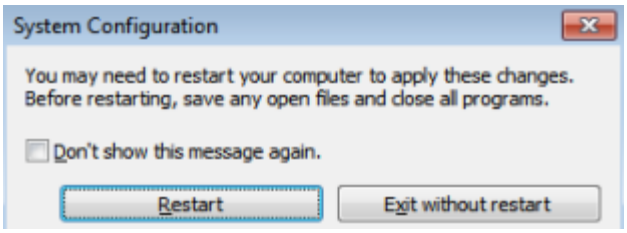
Schritt	Details
Schritt 37: Deaktivieren Sie Windows-Updates.	1 Wählen Sie **Start** | **Systemsteuerung** | **Windows-Update** | **Einstellungen ändern.** 2 Führen Sie auf der Seite **Einstellungen ändern** die folgenden Schritte durch. a Wählen Sie unter **Wichtige Updates** die Option **Nie nach Updates suchen (nicht empfohlen).** b Deaktivieren Sie die Kontrollkästchen unter **Empfohlene Updates, Wer kann Updates installieren?, Microsoft Update, Benachrichtigungen über Software.**  3 Klicken Sie auf **OK**.
Schritt 38: Um Microsoft Word-, Excel- und PowerPoint-Dateien zu analysieren, installieren Sie Microsoft Office 2003 auf dem virtuellen Computer.	

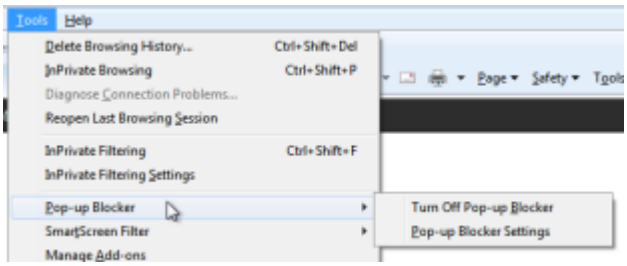
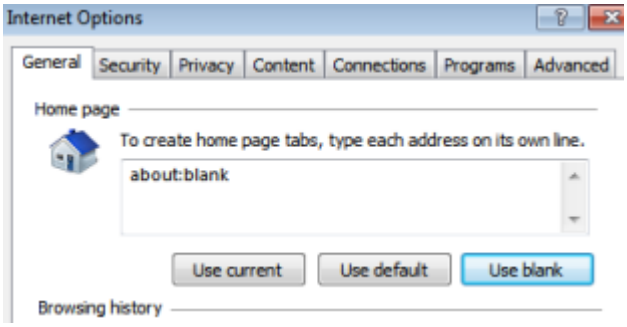
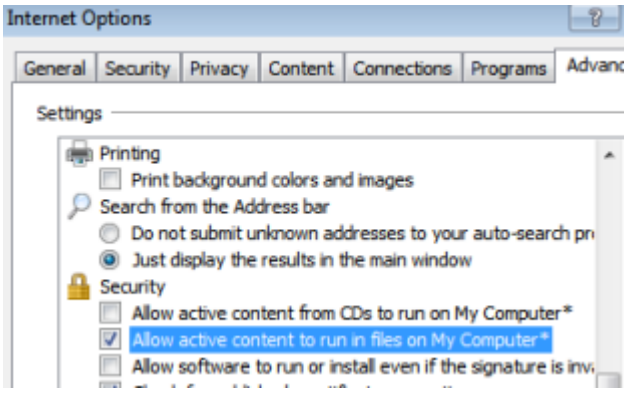
Schritt	Details
Schritt 39: Senken Sie die Sicherheitsstufe, um Makros für Office-Anwendungen auszuführen.	• Öffnen Sie Microsoft Word 2003, und wählen Sie **Extras** | **Makro** | **Sicherheit** und dann **Niedrig**, und klicken Sie auf **OK**.  • Setzen Sie genauso die Makrosicherheit für Microsoft Excel und PowerPoint herab.
Schritt 40: Sie benötigen das Compatibility Pack, um Microsoft Office-Dateien öffnen zu können, die mit einer neueren Version von Microsoft Office erstellt wurden. Beispiel: Zum Öffnen einer DOCX-Datei mit Office 2003 muss das entsprechende Compatibility Pack installiert sein. Rufen Sie http://www.microsoft.com/en-us/download/details.aspx?id=3 auf, und laden Sie das erforderliche Microsoft Office Compatibility Pack für Word-, Excel- und PowerPoint-Dateiformate herunter. Installieren Sie es anschließend auf dem virtuellen Computer. Installieren Sie das Compatibility Pack nach dem Herunterladen auf dem virtuellen Computer. Installieren Sie zum Öffnen der Dateien, die von einer neueren Version von Microsoft Office-Anwendungen erstellt wurden,	

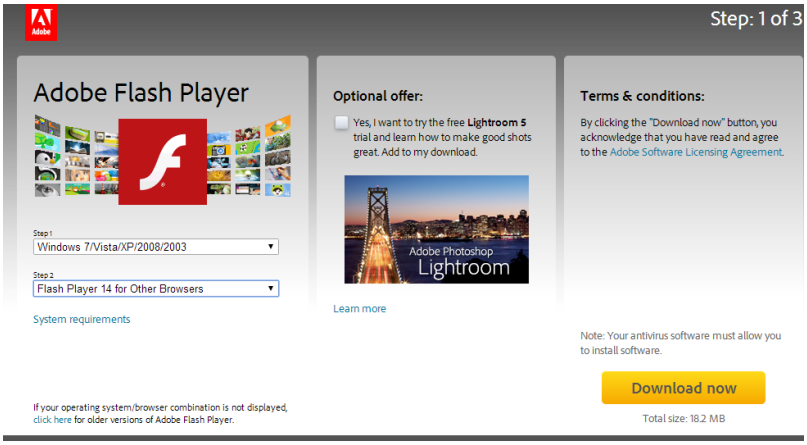
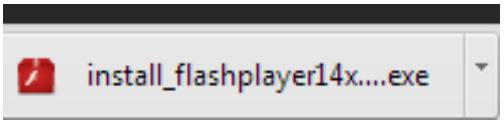
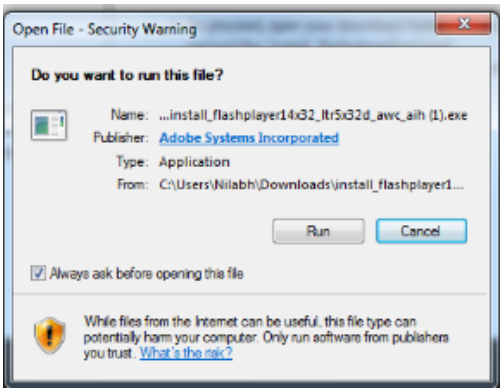
Schritt	Details
Schritt 41: Aktivieren Sie im Dialogfeld **Compatibility Pack für 2007 Office System** die Option **Klicken Sie hier, um den Microsoft-Software-Lizenzbedingungen zuzustimmen**, und klicken Sie auf **Weiter**.	

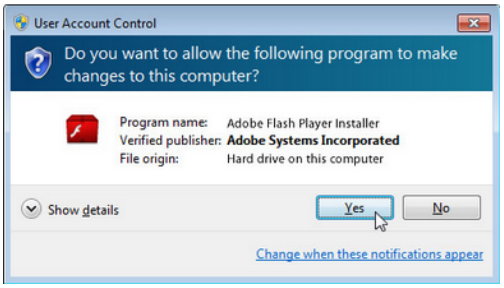
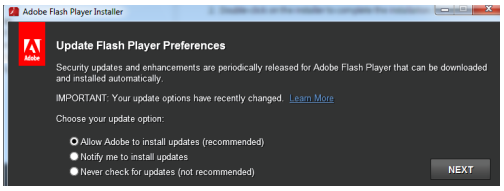
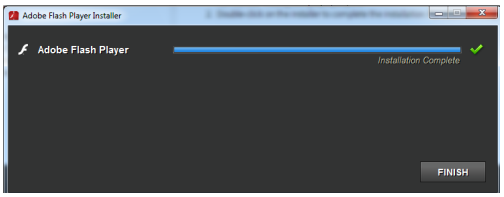
Schritt	Details
Schritt 42: Um PDF-Dateien zu analysieren, laden Sie Adobe Reader auf den nativen Host herunter, und kopieren Sie ihn auf die VM. In diesem Beispiel wird Adobe Reader 9.0 verwendet.	1 Installieren Sie Adobe Reader 9.0 auf der VM. 2 Öffnen Sie Adobe Reader, und klicken Sie auf **Akzeptieren**.  3 Wählen Sie in Adobe Reader **Bearbeiten** | **Voreinstellungen** | **Allgemein** , und deaktivieren Sie **Nach Updates suchen.** 

Schritt	Details
Schritt 43: Laden Sie zum Analysieren von JAR-Dateien Java Runtime Environment herunter, und installieren Sie die Anwendung. In diesem Beispiel wird Java 7 Update 25 verwendet.	
Schritt 44: Öffnen Sie Java in der Systemsteuerung.	
Schritt 45: Deaktivieren Sie auf der Registerkarte **Update** die Option **Automatisch nach Updates suchen.**	

Schritt	Details
Schritt 46: Wählen Sie im Dialogfeld "Java-Update – Warnung" die Option **Nicht überprüfen**, und klicken Sie dann in der Java-Systemsteuerung auf **OK**.	
Schritt 47: Geben Sie im Windows-Dialogfeld "Ausführen" `msconfig` ein.	
Schritt 48: Navigieren Sie im Systemkonfigurationsprogramm zur Registerkarte **Start**.	 Deaktivieren Sie *reader_sl* und *jusched*, und klicken Sie dann auf **OK**.
Schritt 49: Klicken Sie in der **Systemkonfiguration** auf **Neu starten**.	

Schritt	Details
Schritt 50: Öffnen Sie den Standard-Browser, und richten Sie ihn für Malware-Analysen ein. In diesem Beispiel wird Internet Explorer verwendet.	1 Stellen Sie sicher, dass der Popupblocker eingeschaltet ist. Wählen Sie in Internet Explorer **Extras** | **Popupblocker** | **Popupblocker einschalten.**  2 Wählen Sie **Extras** | **Internetoptionen** , und wählen Sie abhängig von der Version von Internet Explorer unter **Startseite** entweder **Leere Seite** oder **Neue Registerkarte** aus.  3 Wechseln Sie zur Registerkarte **Erweitert**, und suchen Sie **Sicherheit.** 4 Wählen Sie **Ausführung aktiver Inhalte in Dateien auf dem lokalen Computer zulassen** aus.  5 Klicken Sie auf **OK.**

Schritt	Details
Schritt 51: Um eine Flash-Datei (SWF) dynamisch zu analysieren, installieren Sie die erforderliche Version von Adobe Flash. In diesem Beispiel wird Flash Player 14 verwendet.	1 Rufen Sie http://get.adobe.com/de/flashplayer/otherversions/ auf. 2 Wählen Sie gemäß Ihren Anforderungen ein Betriebssystem und eine Flash Player-Version in den Dropdown-Menüs **Schritt 1** und **Schritt 2** aus (siehe unten). 3 Klicken Sie auf **Jetzt herunterladen**.  4 Doppelklicken Sie in der unteren Ecke Ihres Bildschirms auf die Installationsdatei für Adobe Flash Player **(install_flashplayer xxx.exe)**.  5 Klicken Sie im Dialogfeld **Sicherheitswarnung** auf **Ausführen**.  6 Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.

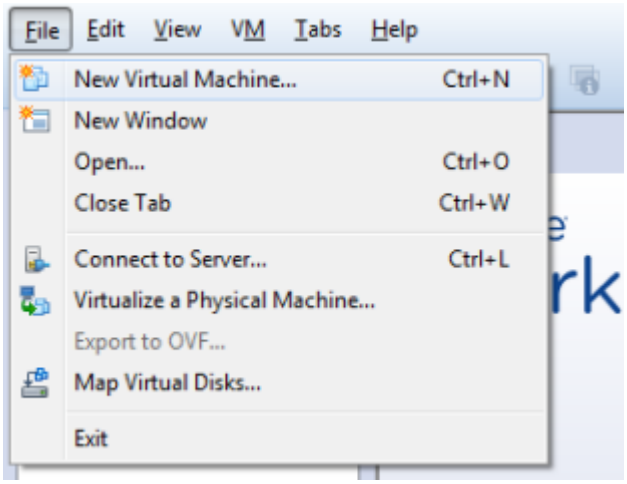
Schritt	Details
	 7 Wählen Sie Ihre Aktualisierungsoption, und klicken Sie auf **WEITER**.  8 Klicken Sie auf **FERTIGSTELLEN**, um die Adobe Flash Player-Installation abzuschließen. 
Schritt 52: Fahren Sie das virtualMachineImage herunter, indem Sie folgende Optionen auswählen: **Start** | **Herunterfahren**.	
Schritt 53: Navigieren Sie zu dem Speicherort, den Sie in Schritt 8 angegeben haben, um die VMDK-Datei mit dem Namen `virtualMachineImage-flat.vmdk` aufzurufen.	

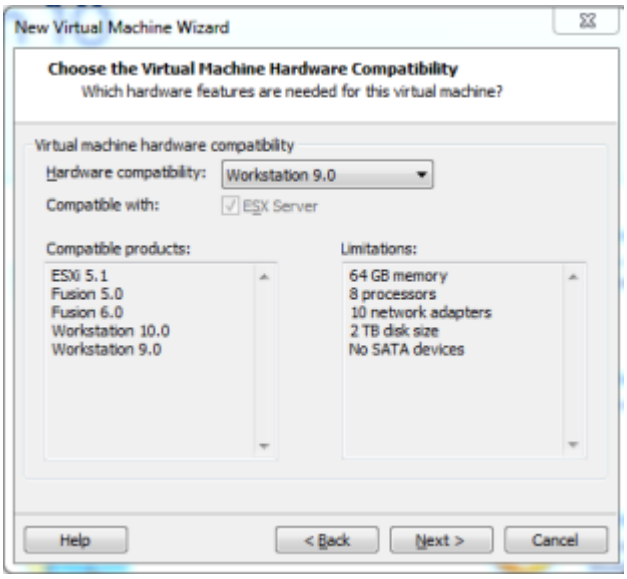
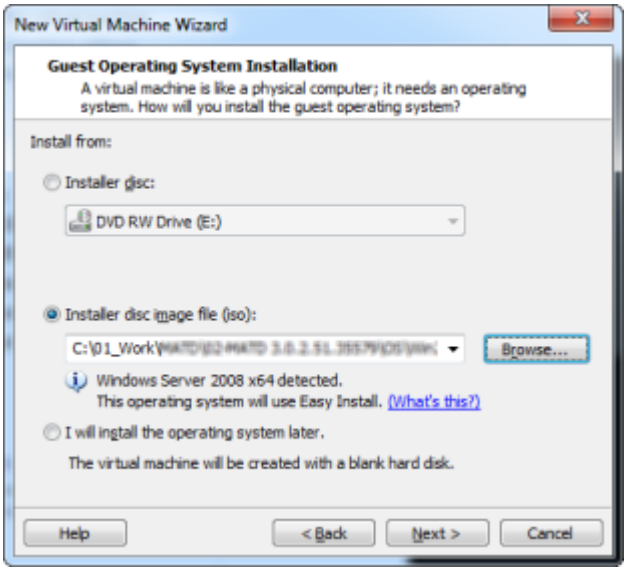
Erstellen einer VMDK-Datei für Windows 2008 Server

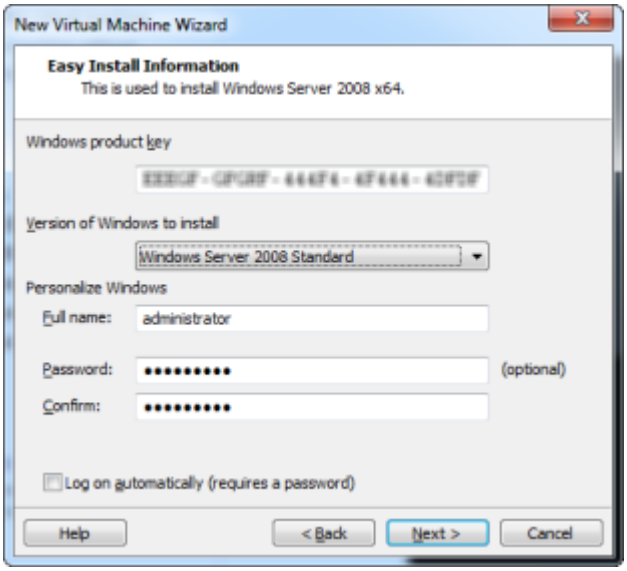
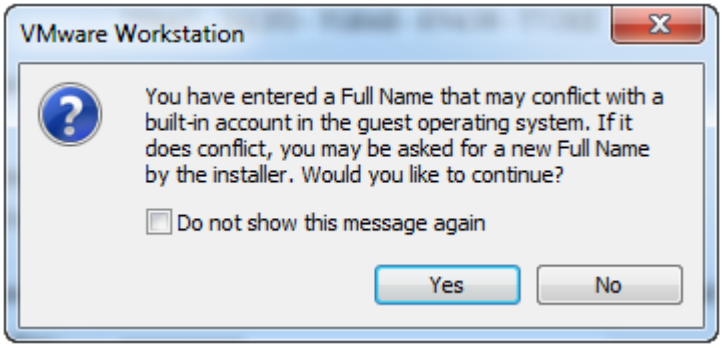
Bevor Sie beginnen

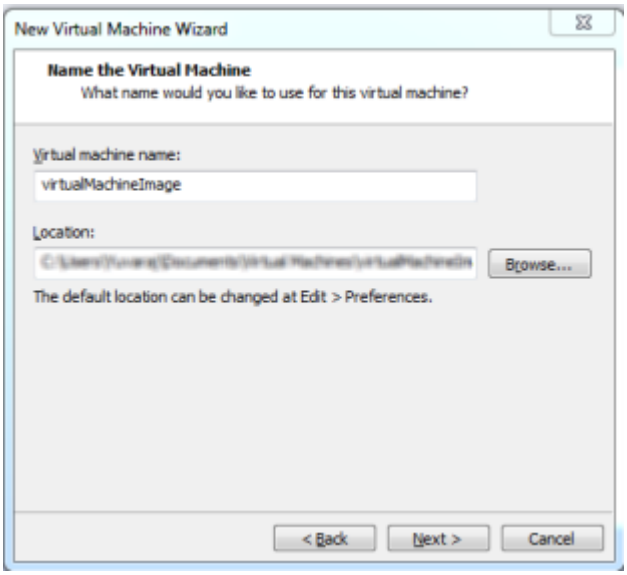
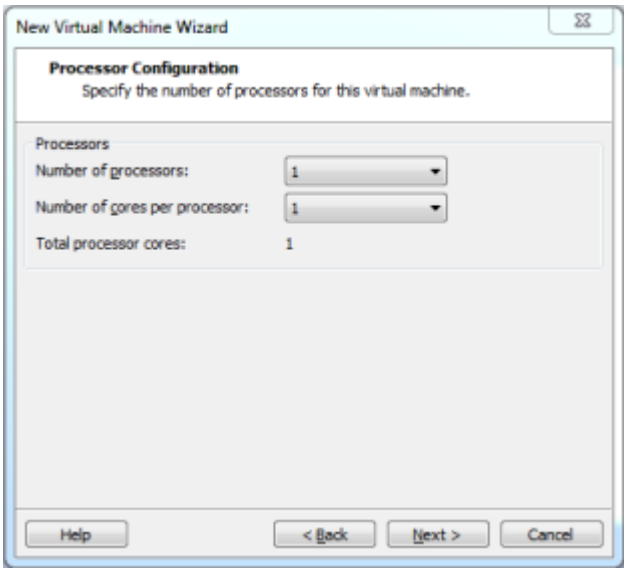
- Laden Sie VMware Workstation 9.0 oder höher von der Seite http://www.vmware.com/products/workstation/workstation-evaluation herunter, und installieren Sie das Programm.
- Stellen Sie sicher, dass Sie über ein ISO-Image von Windows 2008 R2 SP1 verfügen, für das Sie die VMDK-Datei erstellen. Nur Windows 2008 Professional wird unterstützt.
- Stellen Sie sicher, dass Sie über den Lizenzschlüssel für das Betriebssystem verfügen.

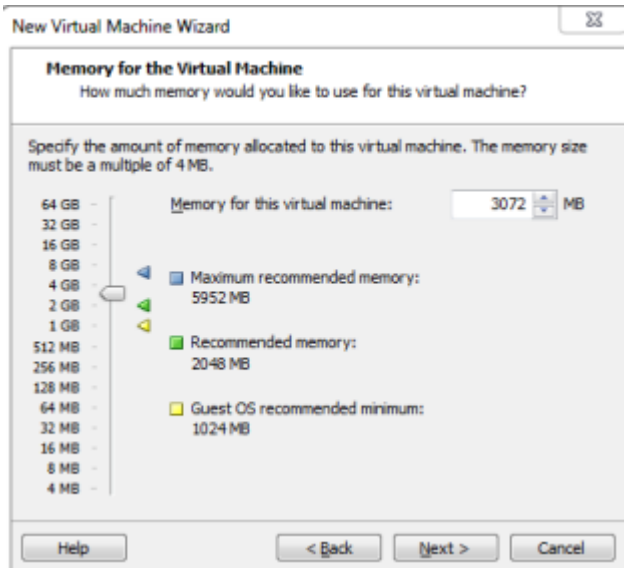
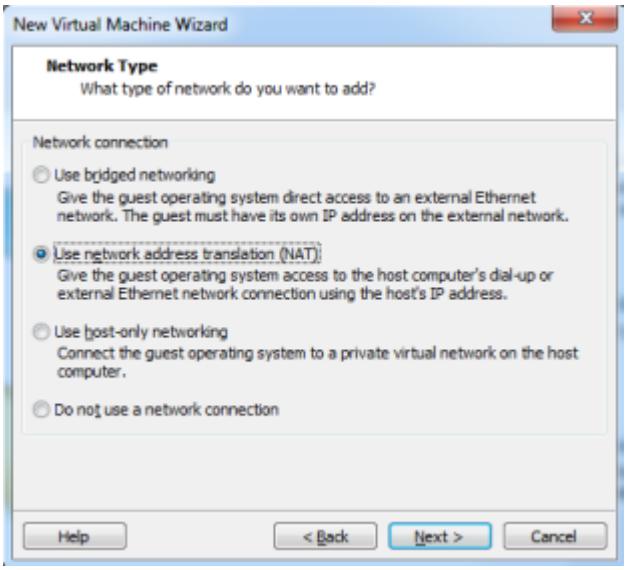
Gehen Sie wie nachfolgend beschrieben vor, um VMDK-Dateien von ISO-Images von Windows 2008 R2 SP1 zu erstellen.

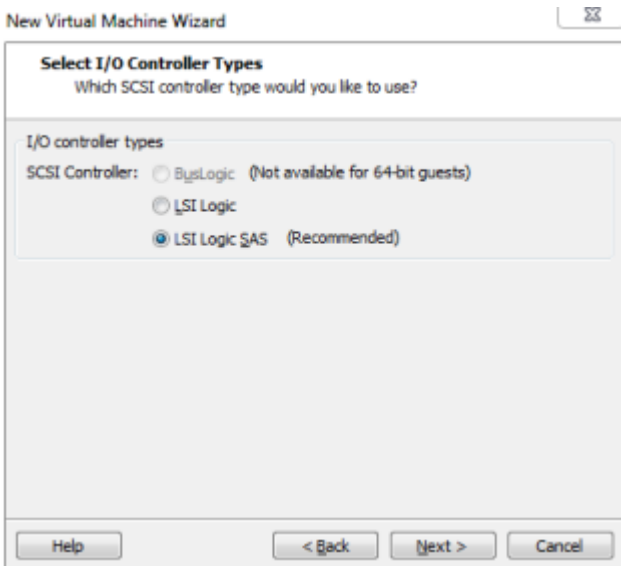
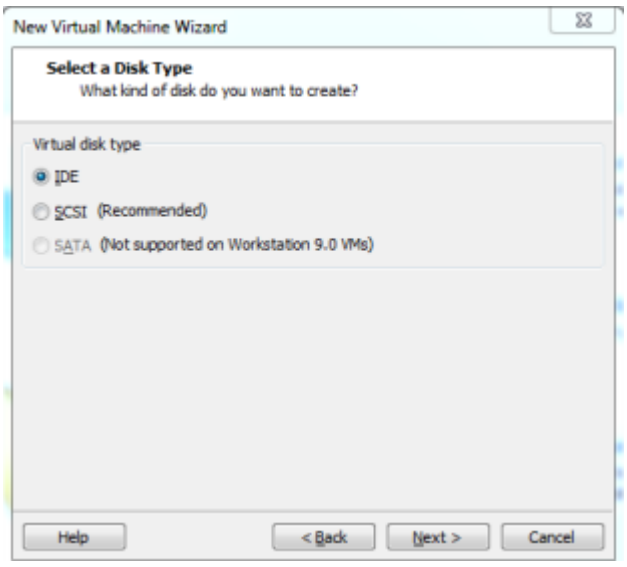
Schritt	Details
Schritt 1: Starten Sie VMware Workstation.	In diesem Beispiel wird VMware Workstation 10 verwendet.
Schritt 2: Wählen Sie auf der VMware Workstation-Seite **Datei | New Virtual Machine (Neuer virtueller Computer)**.	
Schritt 3: Wählen Sie im Fenster **New Virtual Machine Wizard** (Assistent für neue virtuelle Computer) die Option **Custom (Advanced)** (Benutzerdefiniert (erweitert)), und klicken Sie auf **Next** (Weiter).	

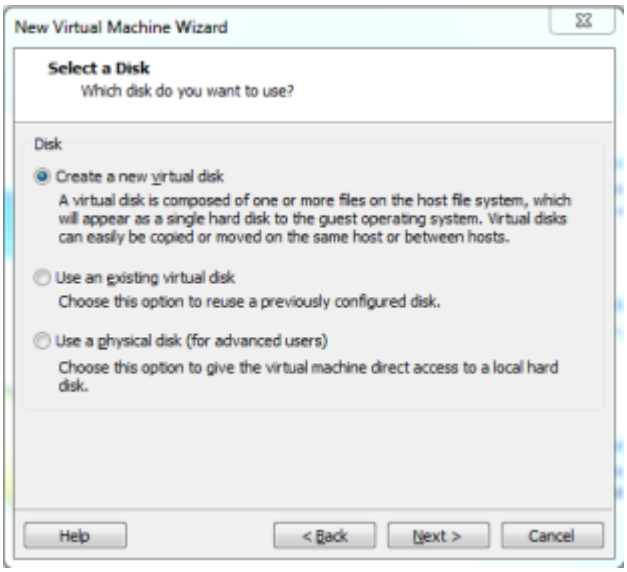
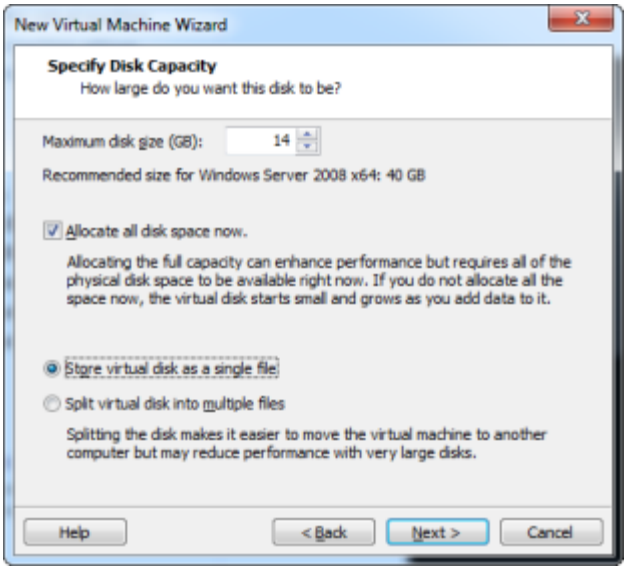
Schritt	Details
Schritt 4: Wählen Sie im Fenster **Choose the Virtual Machine Hardware Compatibility** (Wählen der Hardwarekompatibilität des virtuellen Computers) **Workstation 9.0** aus der Dropdown-Liste **Hardware compatibility** (Hardwarekompatibilität) aus. Akzeptieren Sie bei den anderen Feldern die Standardwerte, und klicken Sie auf **Next** (Weiter).	
Schritt 5: Wählen Sie im Fenster **Guest Operating System Installation** (Installation eines Gast-Betriebssystems) entweder **Installer disc** (Installationsdatenträger) oder **Installer disc image file (iso)** (Image-Datei des Installationsdatenträgers), navigieren Sie zum ISO-Image, wählen Sie es aus, und klicken Sie anschließend auf **Next** (Weiter).	

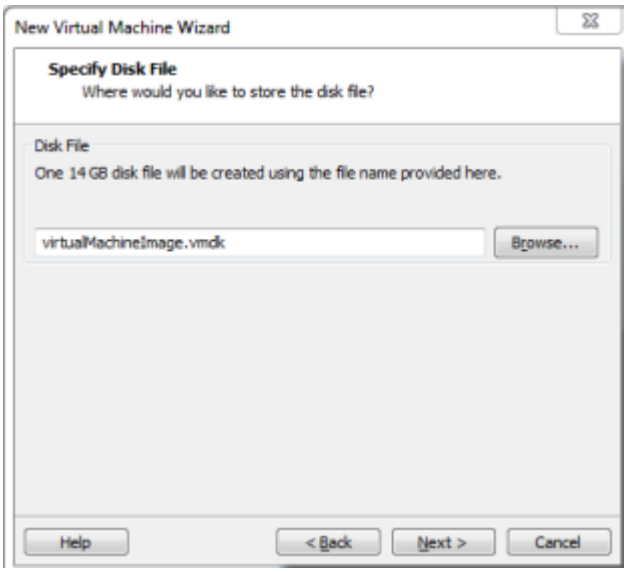
Schritt	Details
Schritt 6: Geben Sie die Informationen im Fenster **Easy Install Information** (Informationen zur einfachen Installation) ein, und klicken Sie auf **Next** (Weiter).	• **Windows product key** (Windows-Produktschlüssel) – Geben Sie den Lizenzschlüssel des Windows-Betriebssystems ein, für das Sie die VMDK-Datei erstellen. • **Version of Windows to install** (Zu installierende Windows-Version) – Wählen Sie die Standard- oder Enterprise-Version. • **Full name** (Vollständiger Name) – Geben Sie `administrator` als **Full name** ein. • **Password** (Kennwort) – Geben Sie `cr@cker42` als Kennwort ein. Dies ist das Kennwort, das McAfee Advanced Threat Defense für die Anmeldung bei der VM verwendet. • **Confirm** (Bestätigen) – Geben Sie `cr@cker42` zur Bestätigung erneut ein. • **Log on automatically (requires a password)** (Automatisch anmelden; Kennwort erforderlich) – Deaktivieren Sie dieses Kontrollkästchen. 
Schritt 7: Klicken Sie im Popupfenster **VMware Workstation** auf **Yes** (Ja).	

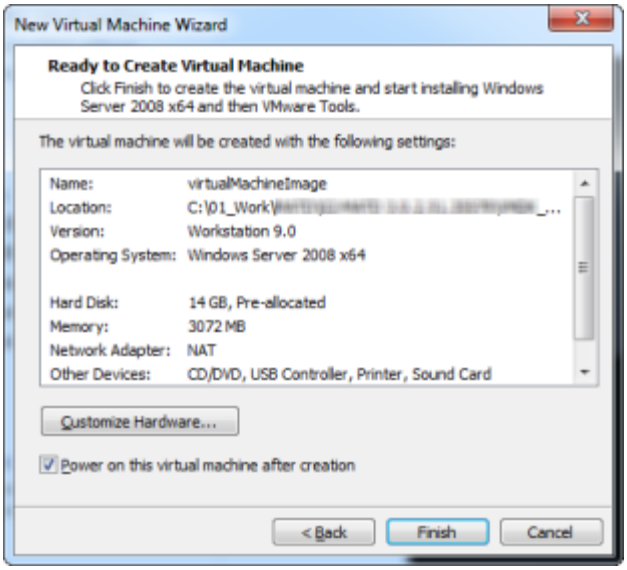
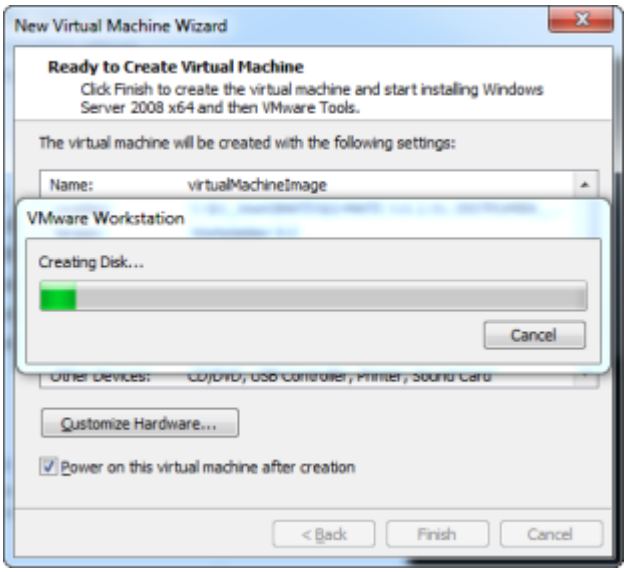
Schritt	Details
Schritt 8: Geben Sie die Informationen im Fenster **Name the Virtual Machine** (Benennen des virtuellen Computers) ein, und klicken Sie anschließend auf **Next** (Weiter).	• **Virtual Machine name** (Name des virtuellen Computers) – Geben Sie `virtualMachineImage` als Namen ein. • **Location** (Speicherort) – Navigieren Sie zu dem Ordner, in dem die VDMK-Datei erstellt werden soll, und wählen Sie ihn aus. 
Schritt 9: Übernehmen Sie im Fenster **Processor Configuration** (Prozessorkonfiguration) die Standardwerte, und klicken Sie auf **Next** (Weiter).	

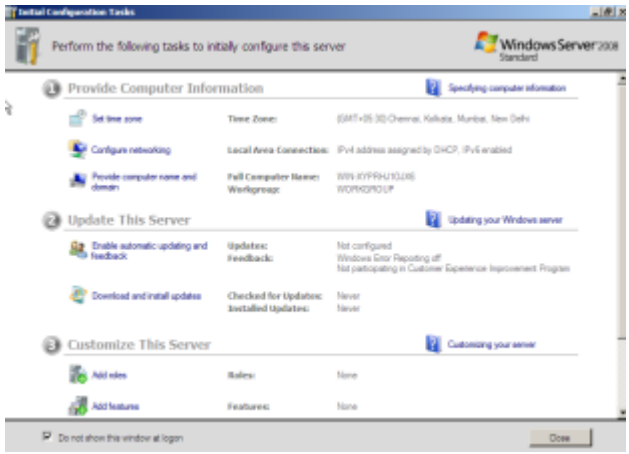
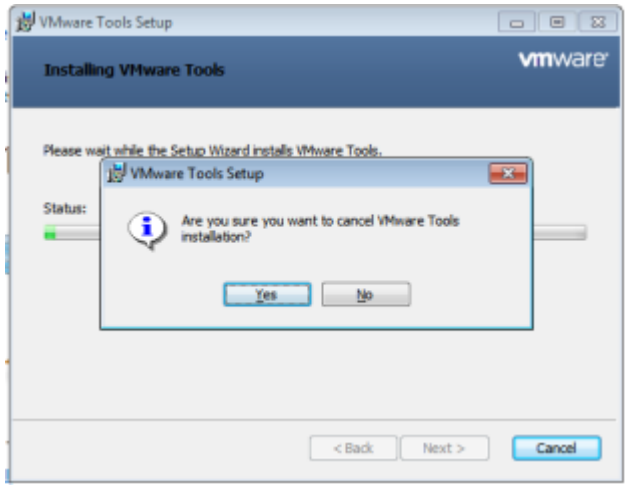
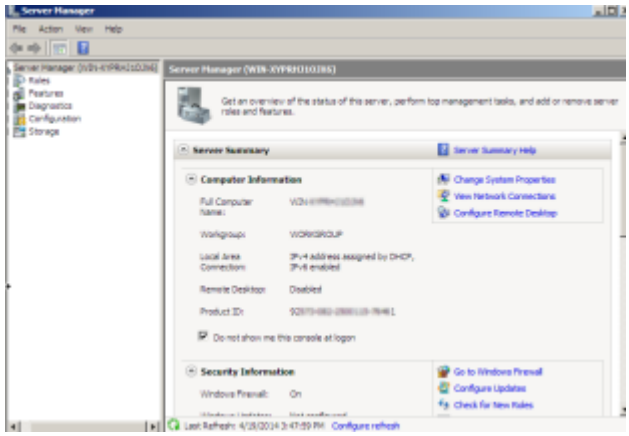
Schritt	Details
Schritt 10: Legen Sie im Fenster **Memory for the Virtual Machine** (Speicher für den virtuellen Computer) 3.072 MB als Speicher fest.	
Schritt 11: Übernehmen Sie im Fenster **Network Type** (Netzwerktyp) die Standardauswahl.	

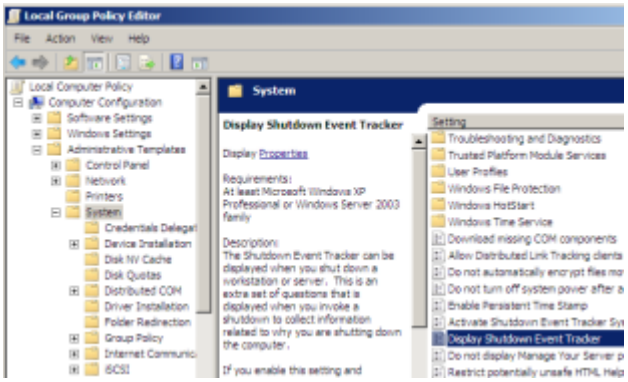
Schritt	Details
Schritt 12: Übernehmen Sie unter **Select I/O Controller Types** (Auswählen der I/O-Controller-Typen) die Standardauswahl.	
Schritt 13: Wählen Sie auf der Seite **Auswählen eines Datenträgertyps** die Option **IDE**, und klicken Sie auf **Next** (Weiter). SCSI-Datenträger sind mit McAfee Advanced Threat Defense nicht kompatibel.	

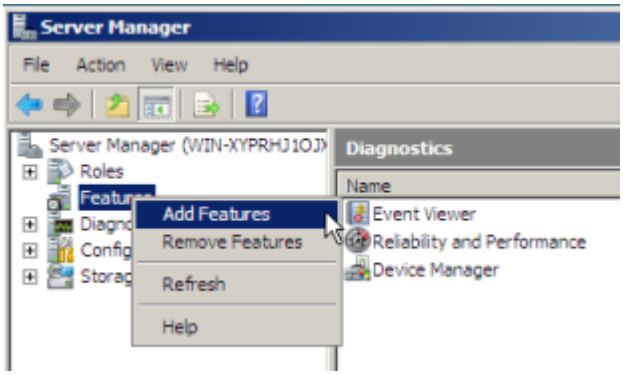
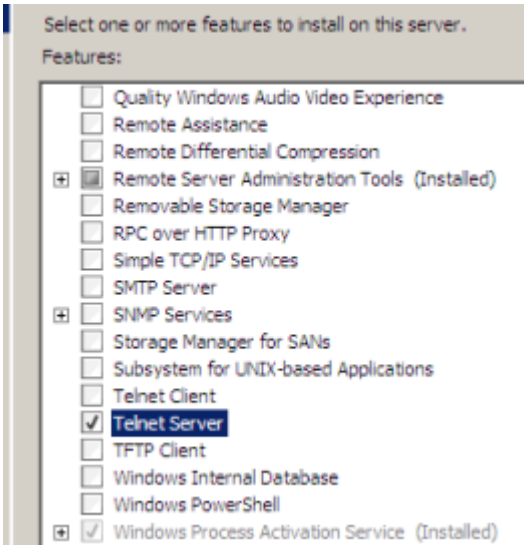
Schritt	Details
Schritt 14: Wählen Sie im Fenster **Auswählen eines Datenträgers** die Option **Create a new virtual disk** (Neuen virtuellen Datenträger erstellen), und klicken Sie auf **Next** (Weiter).	
Schritt 15: Geben Sie die Details im Fenster **Angeben der Speicherkapazität** an, und klicken Sie auf **Next** (Weiter).	• **Maximum disk size (GB)** (Maximale Datenträgergröße in GB) – Geben Sie 14 GB ein. • Wählen Sie **Allocate all disk space now** (Sämtlichen Speicherplatz jetzt zuweisen). • Wählen Sie **Store virtual disk as a single file** (Virtuellen Datenträger als einzelne Datei speichern). 

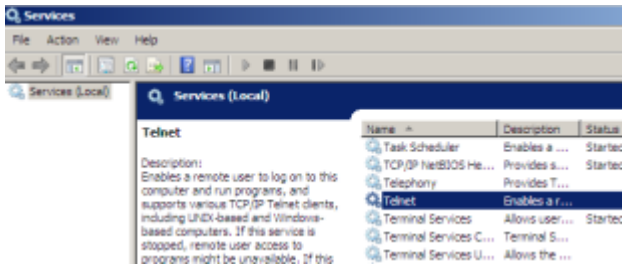
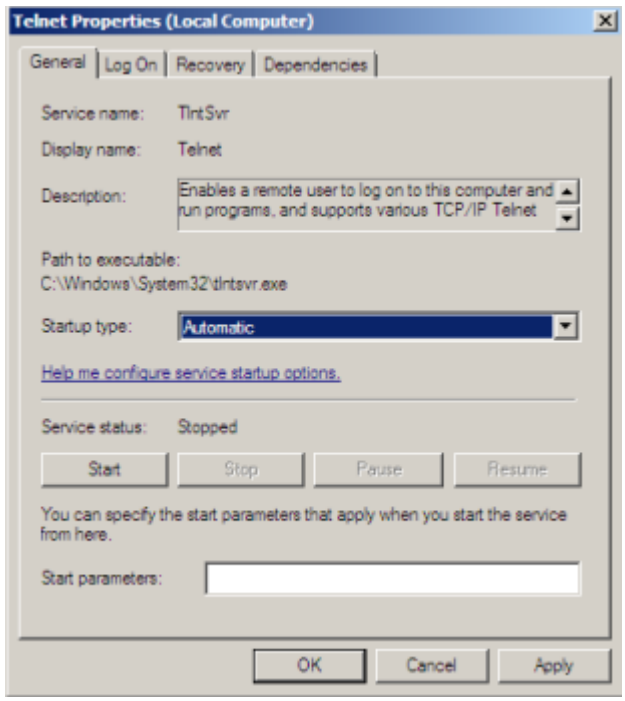
Schritt	Details
Schritt 16: Vergewissern Sie sich, dass im Fenster **Specify Disk file** (Datenträgerdatei angeben) standardmäßig "virtualMachineImage.vmdk" angezeigt wird, und klicken Sie auf **Next** (Weiter). Wenn Sie unter **Virtual Machine name** (Name des virtuellen Computers) einen anderen Namen angegeben haben, wird dieser hier angezeigt.	

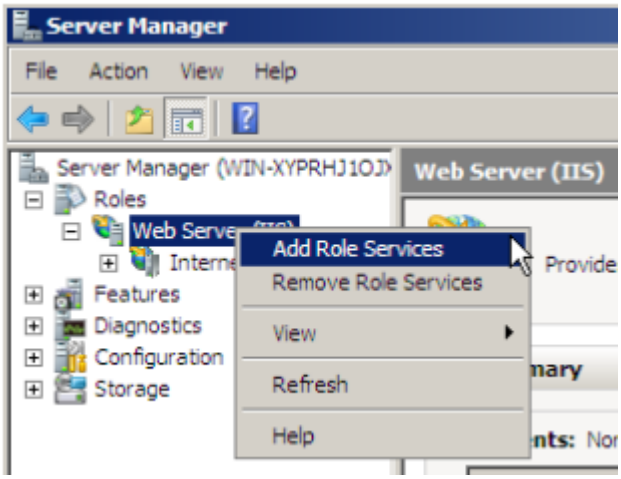
Schritt	Details
Schritt 17: Führen Sie folgende Schritte im Fenster **Ready to Create Virtual Machine** (Bereit zur Erstellung des virtuellen Computers) aus.	• **Power on this virtual machine after creation** (Diesen virtuellen Computer nach der Erstellung einschalten) – Wählen Sie diese Option. • Klicken Sie auf **Finish** (Fertig stellen). Dieser Schritt kann etwa 30 Minuten in Anspruch nehmen.  
Schritt 18: Wenn das Popupfenster **Removable Devices** (Wechselgeräte) angezeigt wird, wählen Sie **Do not show this hint again** (Diesen Hinweis nicht mehr anzeigen), und klicken Sie auf **OK**.	Die Installation von Windows beginnt. Dies kann etwa 15 Minuten dauern.

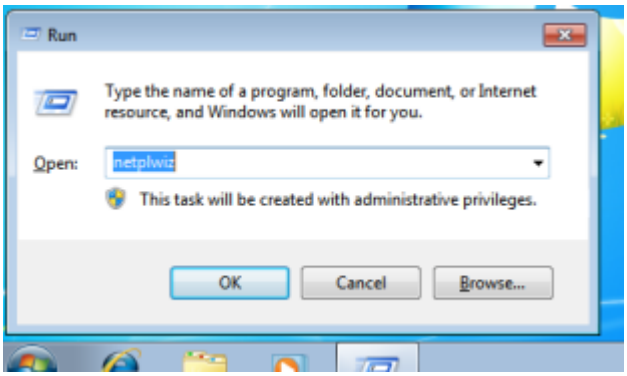
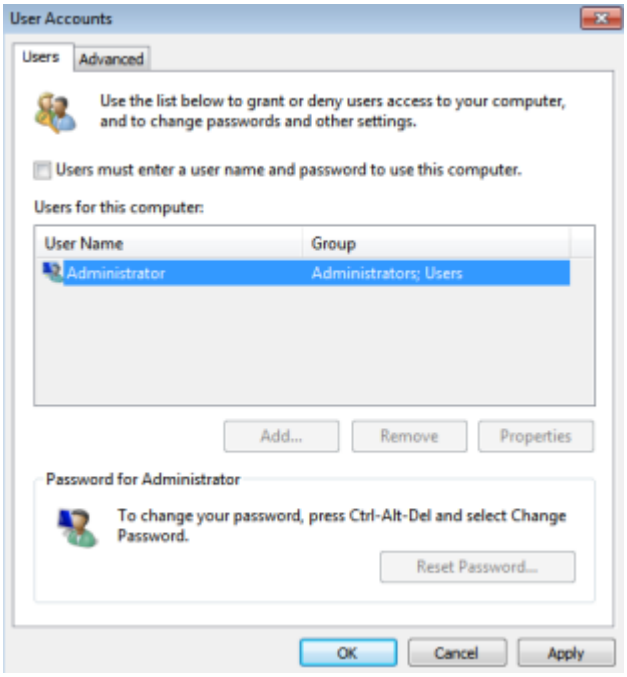
Schritt	Details
Schritt 19: Wenn das Fenster **Aufgaben zur Erstkonfiguration** angezeigt wird, wählen Sie **Dieses Fenster bei der Anmeldung nicht anzeigen**, und klicken Sie auf **Schließen**.	
Schritt 20: Halten Sie die Installation von VMware Tools an. Die VMware Tools sind mit McAfee Advanced Threat Defense nicht kompatibel. Wenn Sie die Installation von VMware Tools nicht angehalten haben, können Sie dennoch mit der VMDK-Dateierstellung fortfahren. Das Programm muss aber deinstalliert sein, sobald die VMDK-Datei bereit ist.	
Schritt 21: Wenn das Fenster **Server-Manager** angezeigt wird, wählen Sie **Diese Konsole bei der Anmeldung nicht mehr anzeigen**, und schließen Sie das Fenster.	

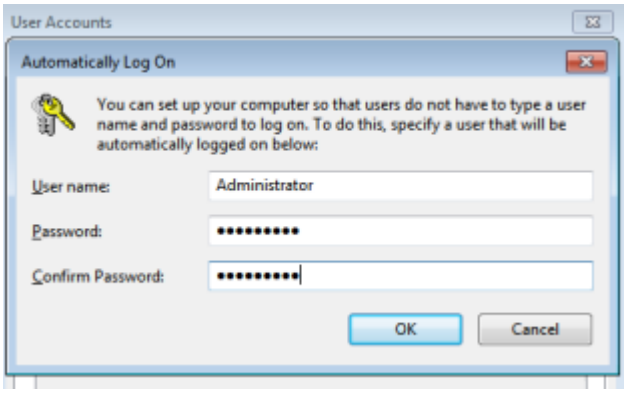
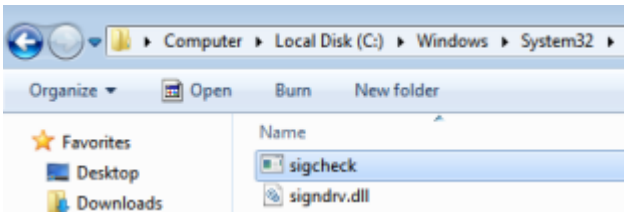
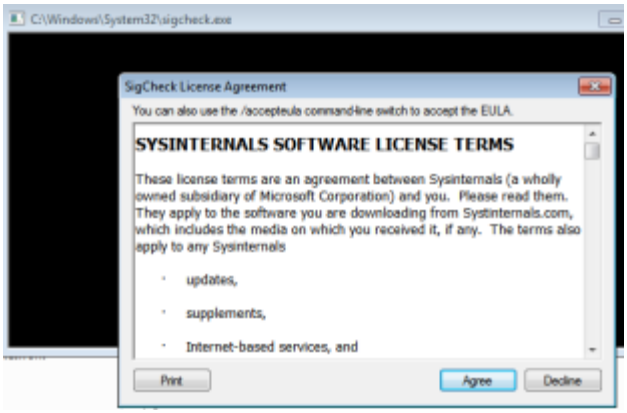
Schritt	Details
Schritt 22: Führen Sie die folgenden Schritte aus.	1 Geben Sie `gpedit.msc` im Windows-Fenster "Ausführen" ein, und drücken Sie die Eingabetaste. 2 Wählen Sie im Fenster **Lokaler Gruppenrichtlinien-Editor** **Computerkonfiguration** | **Administrative Vorlagen** | **System** , und doppelklicken Sie anschließend auf **Ereignisprotokollierung für Herunterfahren anzeigen**.  3 Wählen Sie im Dialogfeld **Eigenschaften von Ereignisprotokollierung für Herunterfahren anzeigen** die Option **Deaktiviert**, und klicken Sie auf **OK**.
Schritt 23: Deaktivieren Sie auf der VM die Windows-Firewall.	1 Wählen Sie **Start** | **Systemsteuerung** | **Windows-Firewall** | **Windows-Firewall ein- oder ausschalten** 2 Wählen Sie **Aus**, und klicken Sie dann auf **OK**.

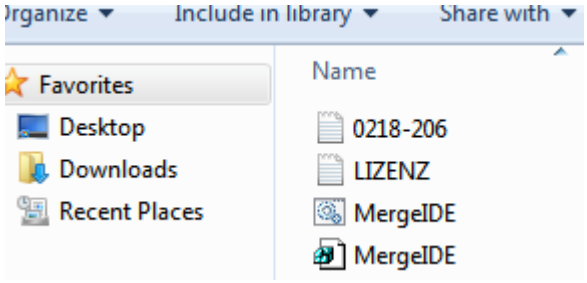
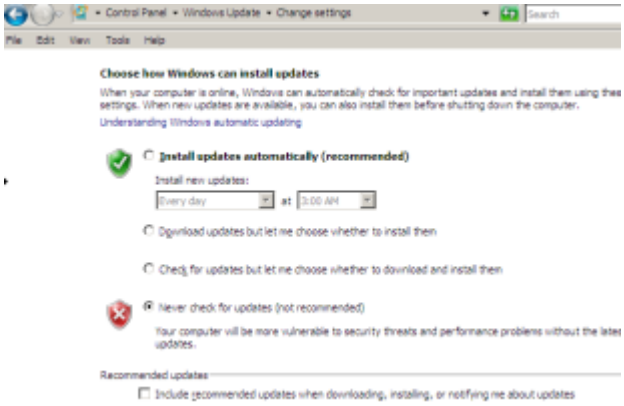
Schritt	Details
Schritt 24: Aktivieren Sie die Telnet-Funktion.	1 Wählen Sie im virtualMachineImage die Optionen **Start** | **Verwaltung** | **Server-Manager**. 2 Klicken Sie im Fenster **Server-Manager** mit der rechten Maustaste auf **Features**, und wählen Sie **Features hinzufügen**.  3 Wählen Sie im **Assistenten "Features hinzufügen"** die Option **Telnet-Server**.  4 Klicken Sie auf **Weiter** und dann auf **Installieren**. 5 Klicken Sie auf **Schließen**, nachdem die Installation erfolgreich durchgeführt wurde.

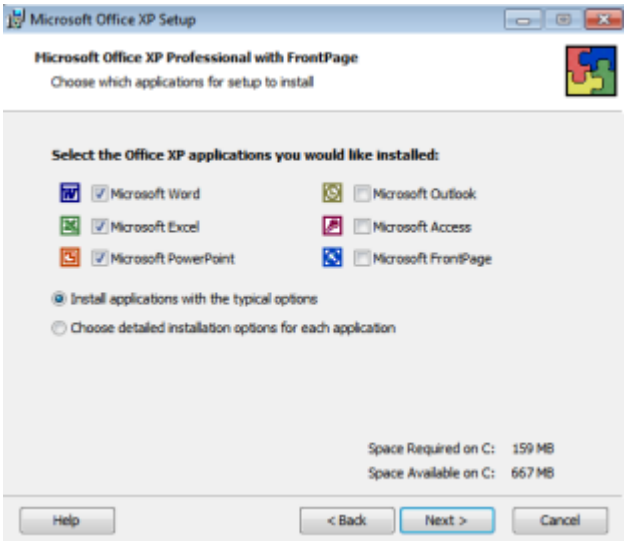
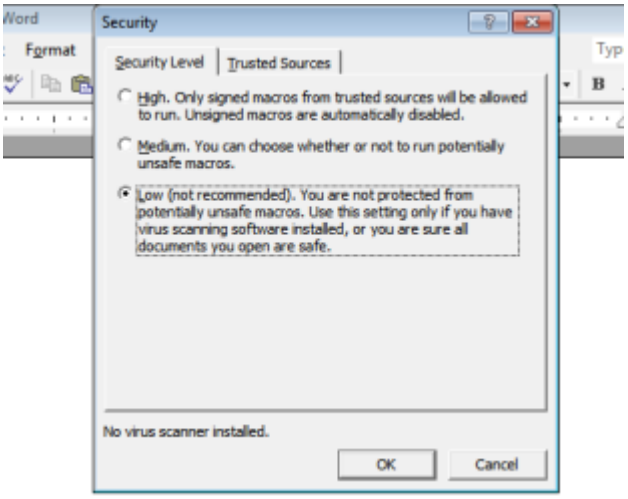
Schritt	Details
Schritt 25: Wählen Sie **Start** | **Verwaltung** | **Dienste.** Doppelklicken Sie anschließend auf **Telnet.**	
Schritt 26: Wählen Sie im Dialogfeld "Eigenschaften von Telnet (Lokaler Computer)" aus der Liste **Starttyp** die Option **Automatisch** aus. Wählen Sie dann **Übernehmen** | **Start** | **OK.**	

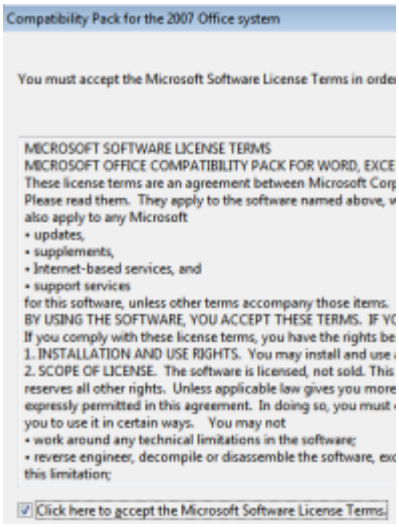
Schritt	Details
Schritt 27: Aktivieren Sie FTP auf der VM.	1 Wählen Sie im virtualMachineImage die Optionen **Start** | **Verwaltung** | **Server-Manager**. 2 Wählen Sie im Fenster **Server-Manager** die Optionen **Server-Manager (Name des virtuellen Computers)** | **Rollen** | **Webserver (IIS)**. 3 Klicken Sie mit der rechten Maustaste auf **Webserver (IIS)**, und wählen Sie **Rollendienste hinzufügen**.  4 Wählen Sie im Assistenten **Rollendienste hinzufügen** die Option **FTP-Publishingdienst**.  Dadurch werden der **FTP-Server** und die **FTP-Verwaltungskonsole** installiert. 5 Klicken Sie auf **Weiter** und dann auf **Installieren**. 6 Klicken Sie auf **Schließen**, nachdem die Installation erfolgreich durchgeführt wurde.

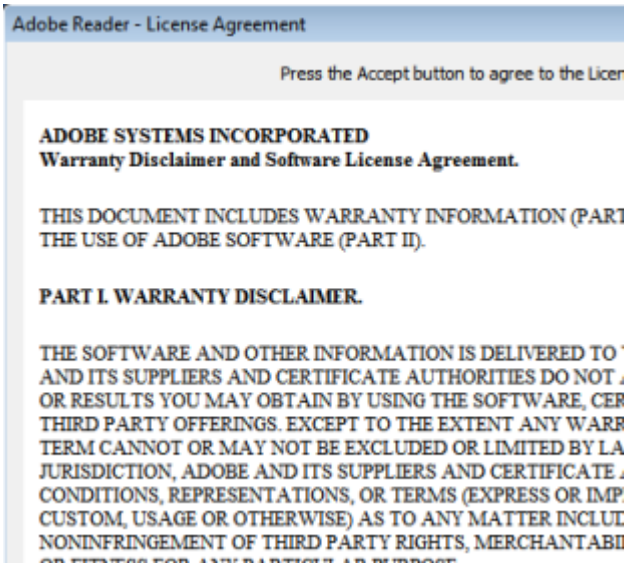
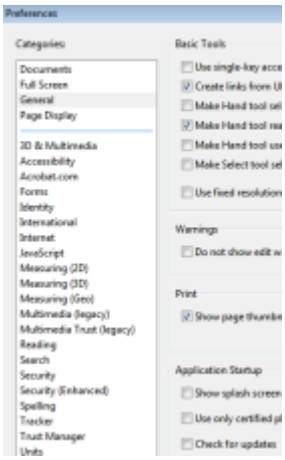
Schritt	Details
Schritt 28: Wählen Sie **Start** | **Ausführen**, geben Sie `netplwiz` ein, und klicken Sie auf **OK**.	
Schritt 29: Deaktivieren Sie im Fenster **Benutzerkonten** die Option **Benutzer müssen Benutzernamen und Kennwort eingeben**, und klicken Sie auf **Übernehmen**.	

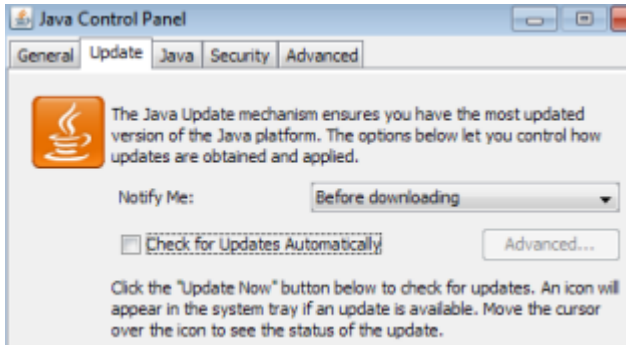
Schritt	Details
Schritt 30: Führen Sie im Popupfenster **Automatische Anmeldung** die folgenden Schritte aus, und klicken Sie dann auf **OK**.	• **Benutzername** – Geben Sie `Administrator` ein. • **Kennwort** – Geben Sie `cr@cker42` ein. • **Kennwort bestätigen** – Geben Sie `cr@cker42` erneut ein. 
Schritt 31: Laden Sie Sigcheck von der Seite http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx auf Ihren Computer (den nativen Host) herunter.	Auf der von Ihnen erstellten VM ist die Windows-Firewall deaktiviert. Außerdem ist kein Virenschutz installiert. Daher wird empfohlen, die Programme und Komponenten zuerst auf den nativen Host herunterzuladen und dann auf die VM in VMware Workstation zu kopieren.
Schritt 32: Extrahieren Sie "sigcheck.zip" an folgendem Speicherort: `C:\WINDOWS\system32`.	
Schritt 33: Navigieren Sie in Windows Explorer zu C:\WINDOWS\system32, und doppelklicken Sie auf **sigcheck.exe**.	
Schritt 34: Klicken Sie im **Sigcheck License Agreement** (Sigcheck-Lizenzvertrag) auf **Agree** (Ich stimme zu). Nach dem Klicken auf **Agree** (Ich stimme zu) wird keine Bestätigungsmeldung angezeigt.	

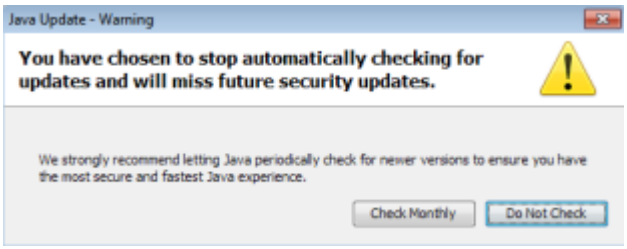
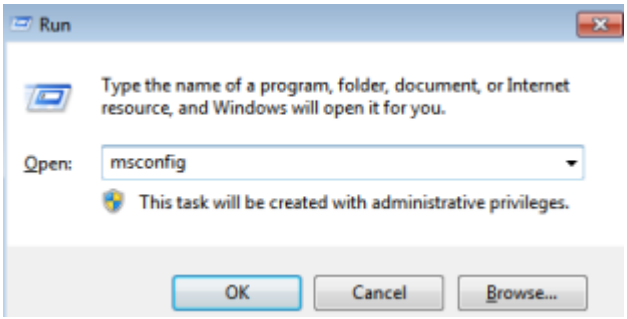
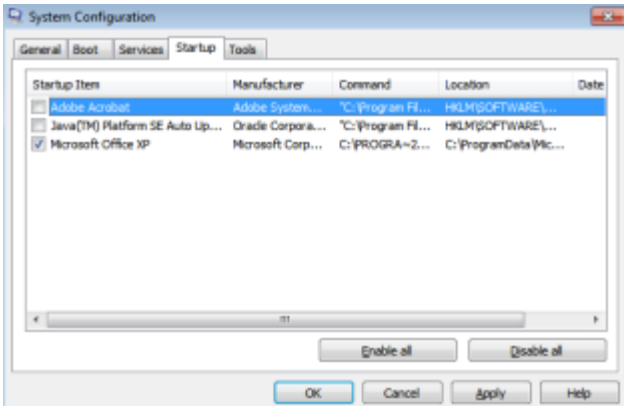
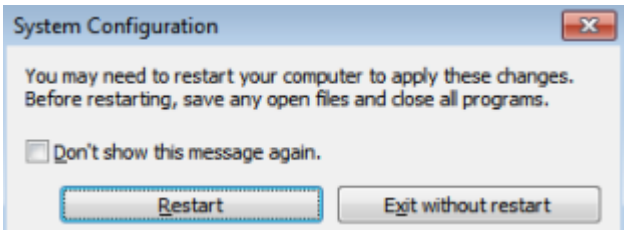
Schritt	Details
Schritt 35: Laden Sie die ZIP-Datei "MergeIDE.zip" von der Seite https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip auf den nativen Computer herunter, und kopieren Sie sie auf die VM.	
Schritt 36: Extrahieren Sie MergeIDE.zip, und führen Sie die MergeIDE-Batchdatei auf der VM aus.	• Klicken Sie in der Warnmeldung auf **Ausführen**, wenn Sie dazu aufgefordert werden. • Schließen Sie Windows Explorer.
Schritt 37: Deaktivieren Sie Windows-Updates.	1 Wählen Sie **Start** | **Systemsteuerung** | **Windows-Update** | **Einstellungen ändern**. 2 Führen Sie auf der Seite **Einstellungen ändern** die folgenden Schritte durch. **a** Wählen Sie **Nie nach Updates suchen (nicht empfohlen)**. **b** Deaktivieren Sie das Kontrollkästchen unter **Empfohlene Updates**.  3 Klicken Sie auf **OK**.

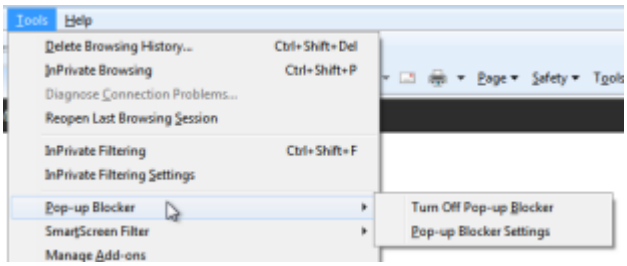
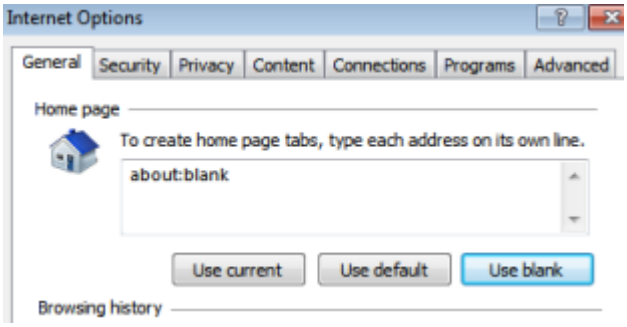
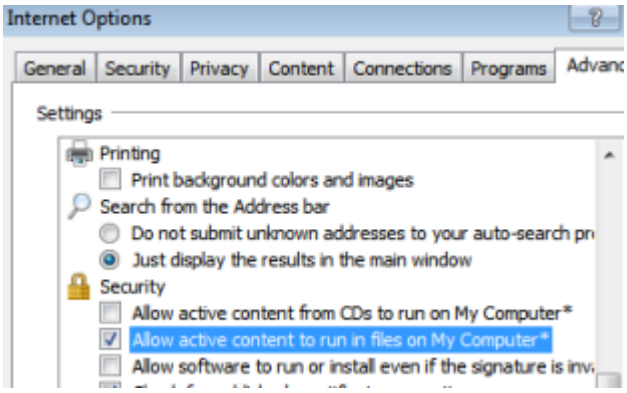
Schritt	Details
Schritt 38: Um Microsoft Word-, Excel- und PowerPoint-Dateien zu analysieren, installieren Sie Microsoft Office 2003 auf dem virtuellen Computer.	
Schritt 39: Senken Sie die Sicherheitsstufe, um Makros für Office-Anwendungen auszuführen.	• Öffnen Sie Microsoft Word 2003, und wählen Sie **Extras** | **Makro** | **Sicherheit** und dann **Niedrig**, und klicken Sie auf **OK**.  • Setzen Sie genauso die Makrosicherheit für Microsoft Excel und PowerPoint herab.

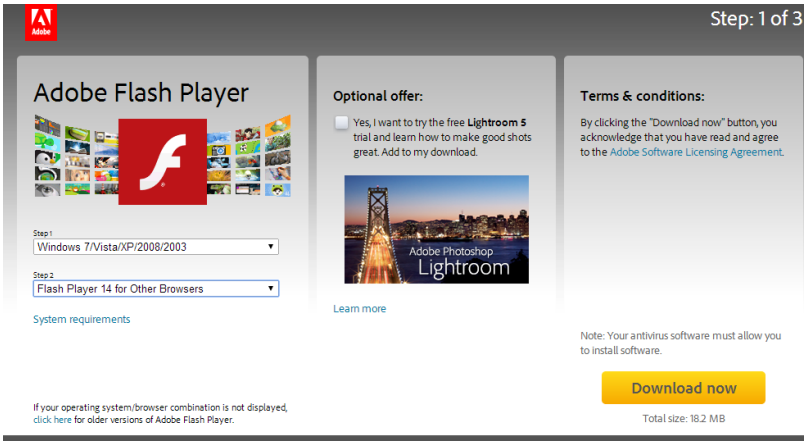
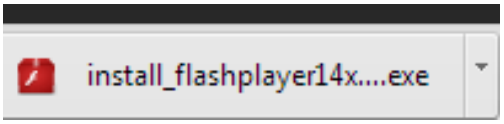
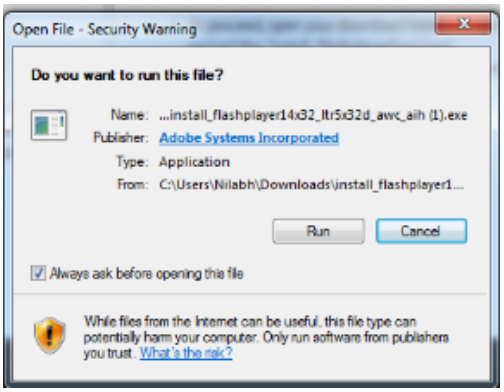
Schritt	Details
Schritt 40: Sie benötigen das Compatibility Pack, um Microsoft Office-Dateien öffnen zu können, die mit einer neueren Version von Microsoft Office erstellt wurden. Beispiel: Zum Öffnen einer DOCX-Datei mit Office 2003 muss das entsprechende Compatibility Pack installiert sein. Rufen Sie http://www.microsoft.com/en-us/download/details.aspx?id=3 auf, und laden Sie das erforderliche Microsoft Office Compatibility Pack für Word-, Excel- und PowerPoint-Dateiformate herunter. Installieren Sie es anschließend auf dem virtuellen Computer.	
Schritt 41: Aktivieren Sie im Dialogfeld **Compatibility Pack für 2007 Office System** die Option **Klicken Sie hier, um den Microsoft-Software-Lizenzbedingungen zuzustimmen**, und klicken Sie auf **Weiter**.	

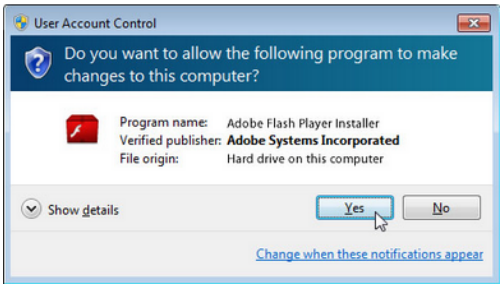
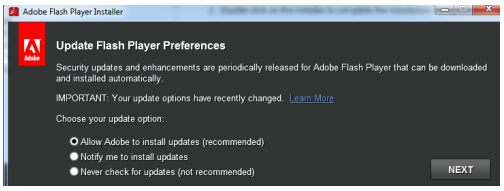
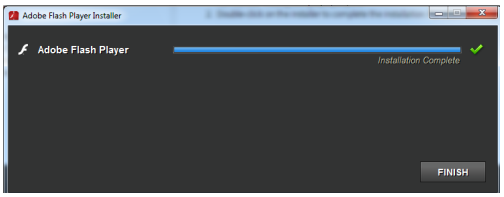
Schritt	Details
Schritt 42: Um PDF-Dateien zu analysieren, laden Sie Adobe Reader auf den nativen Host herunter, und kopieren Sie ihn auf die VM. In diesem Beispiel wird Adobe Reader 9.0 verwendet.	1 Installieren Sie Adobe Reader 9.0 auf der VM. 2 Öffnen Sie Adobe Reader, und klicken Sie auf **Akzeptieren**.  3 Wählen Sie in Adobe Reader **Bearbeiten** | **Voreinstellungen** | **Allgemein** , und deaktivieren Sie **Nach Updates suchen.** 

Schritt	Details
Schritt 43: Laden Sie zum Analysieren von JAR-Dateien Java Runtime Environment herunter, und installieren Sie die Anwendung. In diesem Beispiel wird Java 7 Update 25 verwendet.	
Schritt 44: Öffnen Sie Java in der Systemsteuerung.	
Schritt 45: Deaktivieren Sie auf der Registerkarte **Update** die Option **Automatisch nach Updates suchen.**	

Schritt	Details
Schritt 46: Wählen Sie im Dialogfeld "Java-Update – Warnung" die Option **Nicht überprüfen**, und klicken Sie dann in der Java-Systemsteuerung auf **OK**.	
Schritt 47: Geben Sie im Windows-Dialogfeld "Ausführen" `msconfig` ein.	
Schritt 48: Navigieren Sie im Systemkonfigurationsprogramm zur Registerkarte **Start**.	 Deaktivieren Sie alle Einträge, und klicken Sie auf **OK**.
Schritt 49: Aktivieren Sie im Dialogfeld **Systemkonfiguration** das Kontrollkästchen **Diese Meldung nicht mehr anzeigen**, und klicken Sie auf **Neu starten**.	

Schritt	Details
Schritt 50: Öffnen Sie den Standard-Browser, und richten Sie ihn für Malware-Analysen ein. In diesem Beispiel wird Internet Explorer verwendet.	1 Stellen Sie sicher, dass der Popupblocker ausgeschaltet ist. Wählen Sie in Internet Explorer **Extras** | **Popupblocker** | **Popupblocker ausschalten.**  2 Wählen Sie **Extras** | **Internetoptionen** , und wählen Sie abhängig von der Version von Internet Explorer unter **Startseite** entweder **Leere Seite** oder **Neue Registerkarte** aus.  3 Wechseln Sie zur Registerkarte **Erweitert**, und suchen Sie **Sicherheit**. 4 Wählen Sie **Ausführung aktiver Inhalte in Dateien auf dem lokalen Computer zulassen** aus.  5 Klicken Sie auf **OK**.

Schritt	Details
Schritt 51: Um eine Flash-Datei (SWF) dynamisch zu analysieren, installieren Sie die erforderliche Version von Adobe Flash. In diesem Beispiel wird Flash Player 14 verwendet.	1 Rufen Sie http://get.adobe.com/de/flashplayer/otherversions/ auf. 2 Wählen Sie gemäß Ihren Anforderungen ein Betriebssystem und eine Flash Player-Version in den Dropdown-Menüs **Schritt 1** und **Schritt 2** aus (siehe unten). 3 Klicken Sie auf **Jetzt herunterladen**.  4 Doppelklicken Sie in der unteren Ecke Ihres Bildschirms auf die Installationsdatei für Adobe Flash Player **(install_flashplayer xxx.exe)**.  5 Klicken Sie im Dialogfeld **Sicherheitswarnung** auf **Ausführen**.  6 Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.

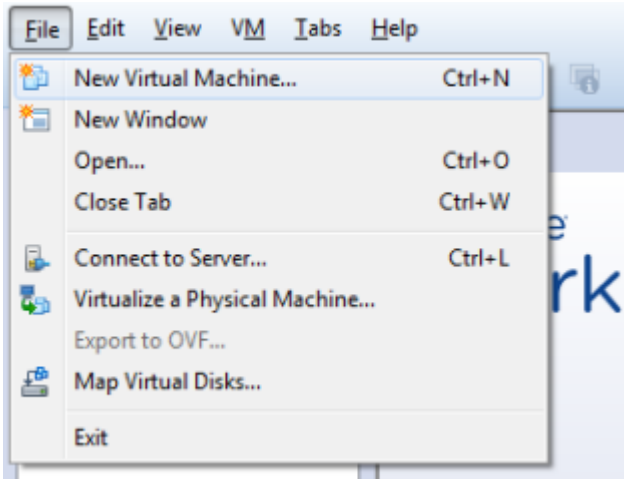
Schritt	Details
	 7 Wählen Sie Ihre Aktualisierungsoption, und klicken Sie auf **WEITER**.  8 Klicken Sie auf **FERTIGSTELLEN**, um die Adobe Flash Player-Installation abzuschließen. 
Schritt 52: Fahren Sie das virtualMachineImage herunter, indem Sie folgende Optionen auswählen: **Start** | **Herunterfahren**.	
Schritt 53: Navigieren Sie zu dem Speicherort, den Sie in Schritt 8 angegeben haben, um die VMDK-Datei mit dem Namen `virtualMachineImage-flat.vmdk` aufzurufen.	

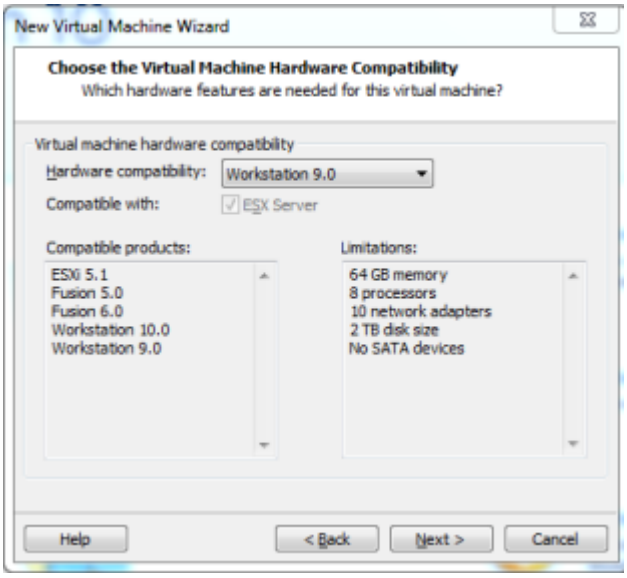
Erstellen einer VMDK-Datei für Windows 8

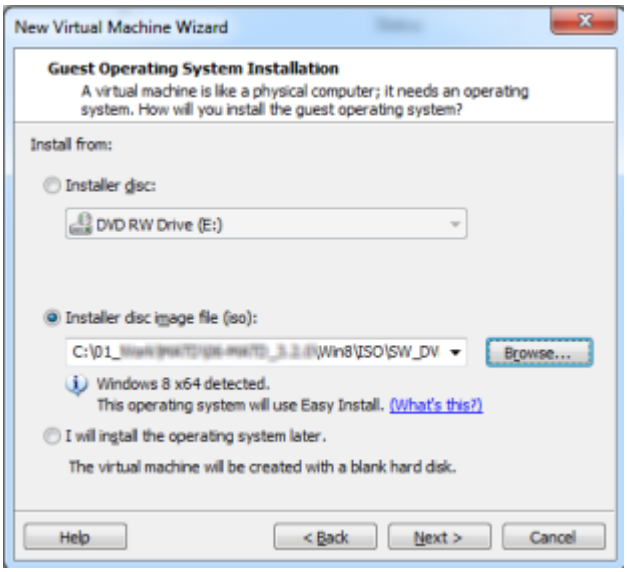
Bevor Sie beginnen

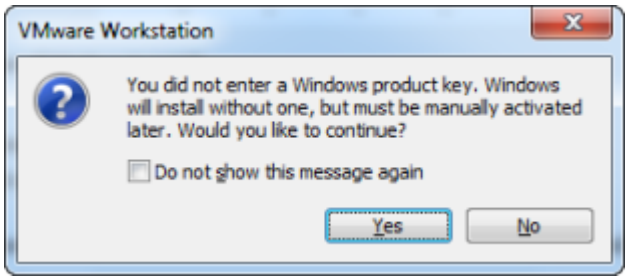
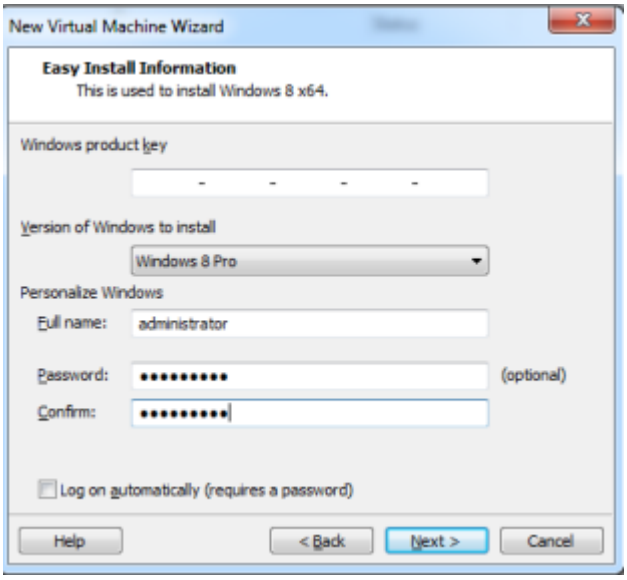
- Laden Sie VMware Workstation 9.0 oder höher von der Seite http://www.vmware.com/products/workstation/workstation-evaluation herunter, und installieren Sie das Programm. McAfee empfiehlt Version 9 oder 10.
- Stellen Sie sicher, dass Sie über ein ISO-Image von Windows 8 32 Bit oder 64 Bit verfügen, für das Sie die VMDK-Datei erstellen müssen. Nur Windows 8 Pro wird unterstützt. Bei diesem Vorgang wird Windows 8 Pro (englische Version) als Beispiel verwendet.
- Stellen Sie sicher, dass Sie über alle notwendigen Informationen basierend auf Ihrem Lizenztyp verfügen, um das Betriebssystem zu aktivieren. Sie müssen erst das Betriebssystem aktivieren, bevor Sie die VMDK-Datei in McAfee Advanced Threat Defense importieren können.

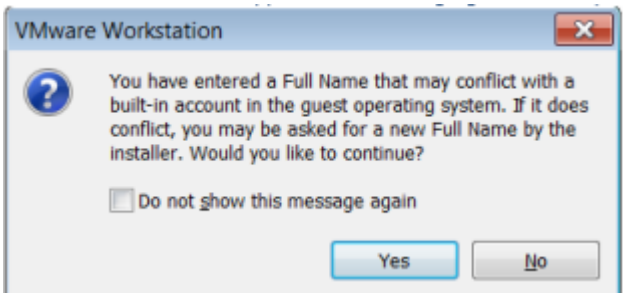
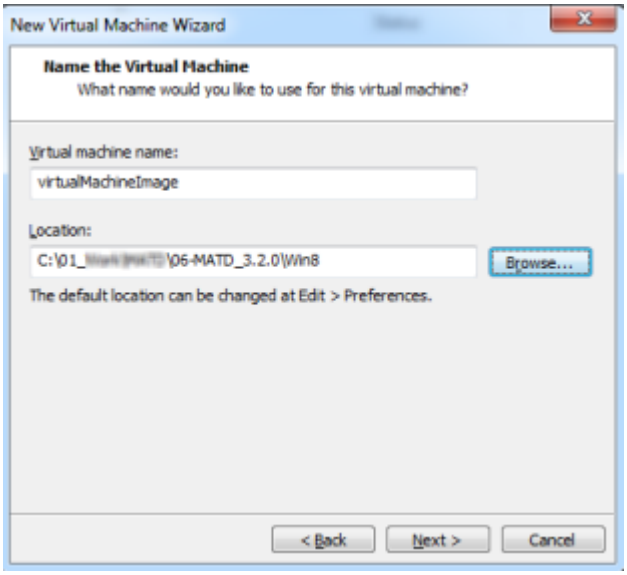
Gehen Sie wie nachfolgend beschrieben vor, um VMDK-Dateien von einem ISO-Image von Windows 8 Pro 32 oder 64 Bit zu erstellen.

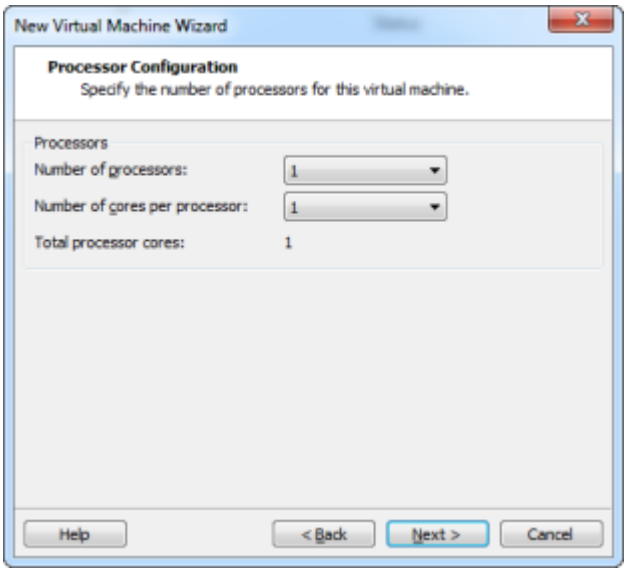
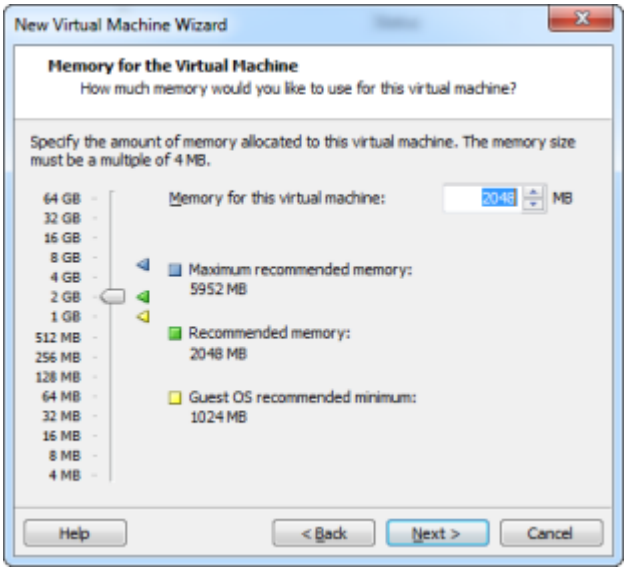
Schritt	Details
Schritt 1: Starten Sie VMware Workstation.	In diesem Beispiel wird VMware Workstation 10 verwendet.
Schritt 2: Wählen Sie auf der VMware Workstation-Seite **Datei** | **New Virtual Machine (Neuer virtueller Computer)**.	

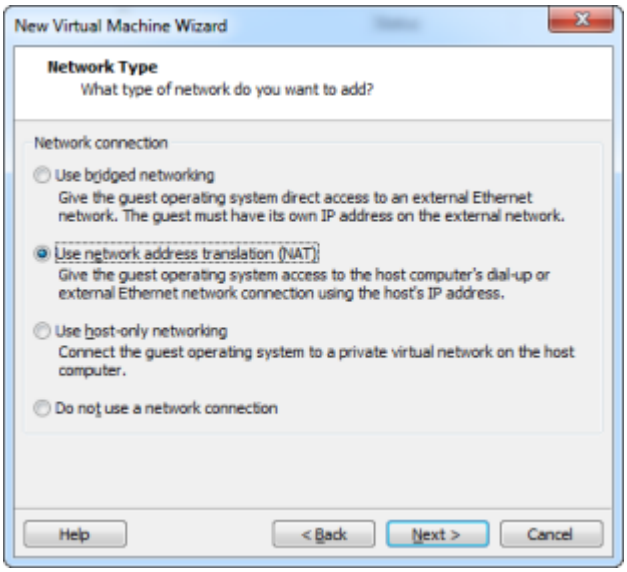
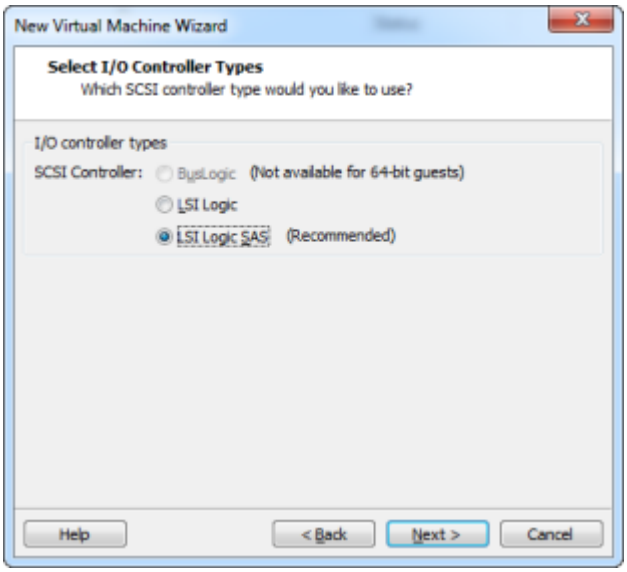
Schritt	Details
Schritt 3: Wählen Sie im Fenster **New Virtual Machine Wizard** (Assistent für neue virtuelle Computer) die Option **Custom (Advanced)** (Benutzerdefiniert (erweitert)), und klicken Sie auf **Next** (Weiter).	
Schritt 4: Wählen Sie im Fenster **Choose the Virtual Machine Hardware Compatibility** (Wählen der Hardwarekompatibilität des virtuellen Computers) **Workstation 9.0** aus der Dropdown-Liste **Hardware compatibility** (Hardwarekompatibilität) aus. Akzeptieren Sie bei den anderen Feldern die Standardwerte, und klicken Sie auf **Next** (Weiter).	

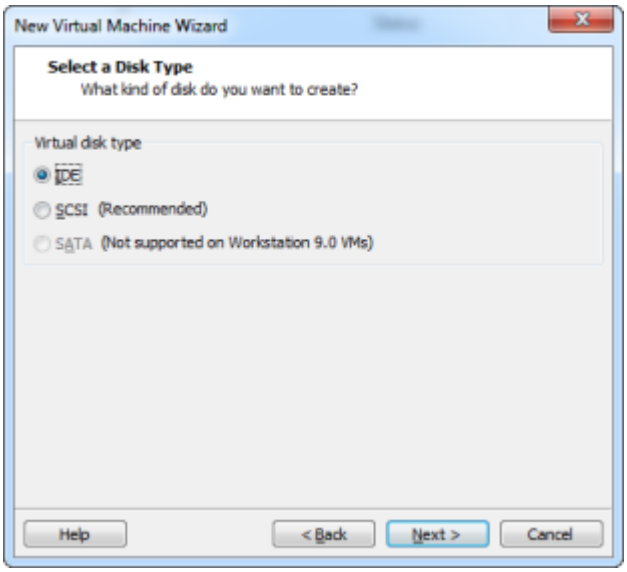
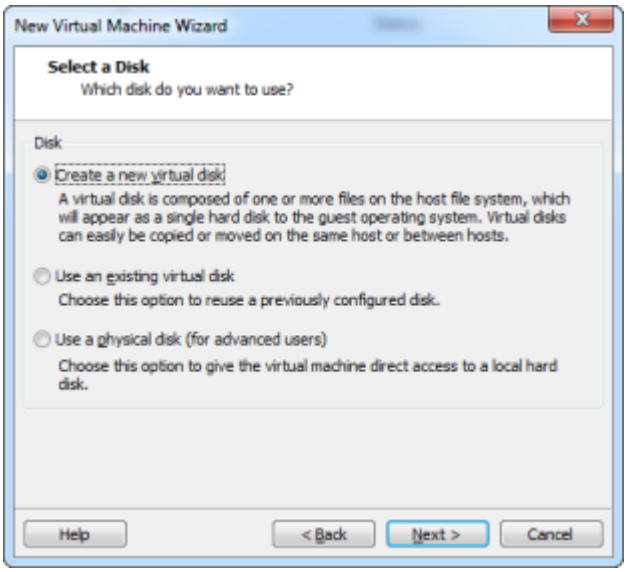
Schritt	Details
Schritt 5: Wählen Sie im Fenster **Guest Operating System Installation** (Installation eines Gast-Betriebssystems) die Option **Installer disc image file (iso)** (Image-Datei des Installationsdatenträgers), navigieren Sie zum ISO-Image, wählen Sie es aus, und klicken Sie anschließend auf **Next** (Weiter).	

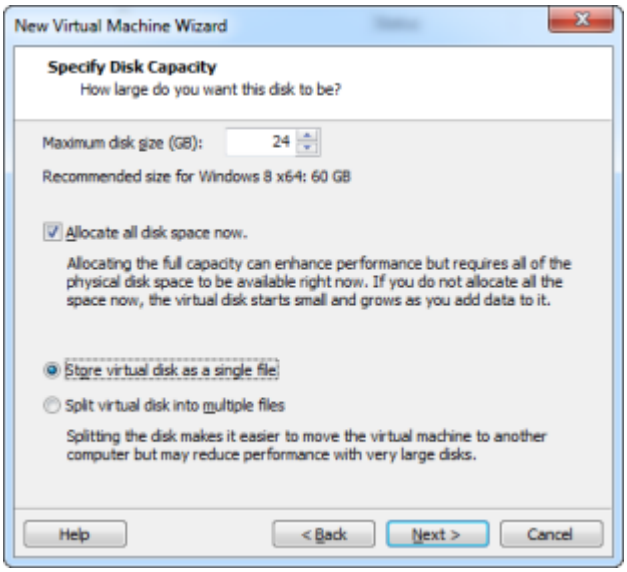
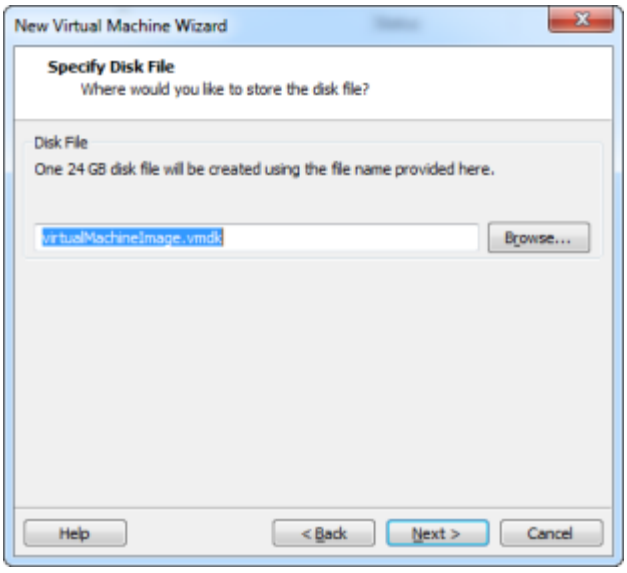
Schritt	Details
Schritt 6: Geben Sie die Informationen im Fenster **Easy Install Information** (Informationen zur einfachen Installation) ein, und klicken Sie auf **Next** (Weiter).	• **Windows product key** (Windows-Produktschlüssel) – Geben Sie den Lizenzschlüssel des Windows-Betriebssystems ein, für das Sie die VMDK-Datei erstellen. Bei einer Volumenlizenz können Sie das Feld leer lassen. Klicken Sie auf **Ja**, wenn die folgende Meldung anschließend angezeigt wird.  • **Full name** (Vollständiger Name) – Geben Sie `administrator` als **Full name** ein. • **Password** (Kennwort) – Geben Sie `cr@cker42` als Kennwort ein. McAfee Advanced Threat Defense verwendet dieses Kennwort zur Anmeldung bei der VM. • **Confirm** (Bestätigen) – Geben Sie `cr@cker42` zur Bestätigung erneut ein. • **Log on automatically (requires a password)** (Automatisch anmelden; Kennwort erforderlich) – Deaktivieren Sie dieses Kontrollkästchen. 

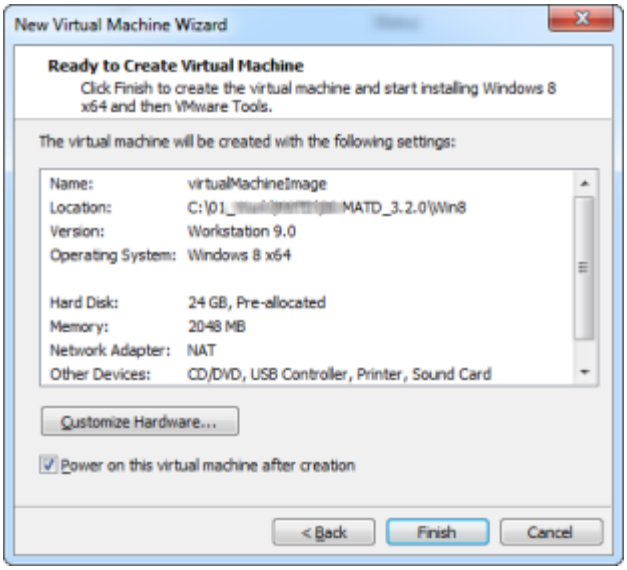
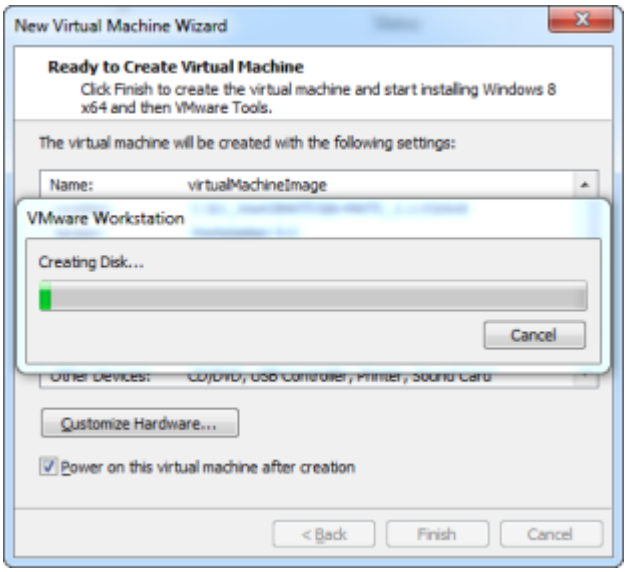
Schritt	Details
Schritt 7: Klicken Sie im Popupfenster **VMware Workstation** auf **Yes** (Ja).	
Schritt 8: Geben Sie die Informationen im Fenster **Name the Virtual Machine** (Benennen des virtuellen Computers) ein, und klicken Sie anschließend auf **Next** (Weiter).	• **Virtual Machine name** (Name des virtuellen Computers) – Geben Sie `virtualMachineImage` als Namen ein. • **Location** (Speicherort) – Navigieren Sie zu dem Ordner, in dem die VDMK-Datei erstellt werden soll, und wählen Sie ihn aus. 

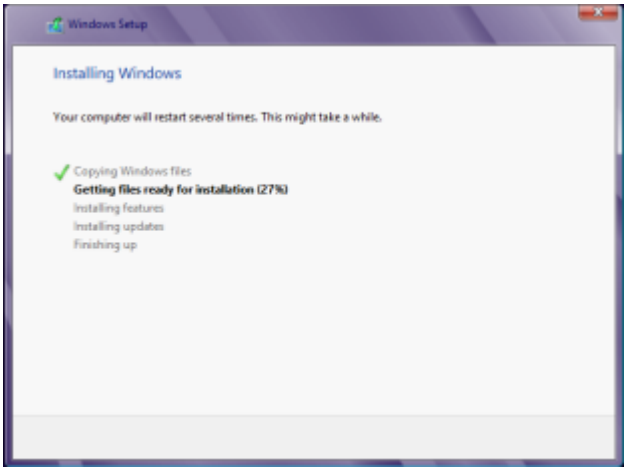
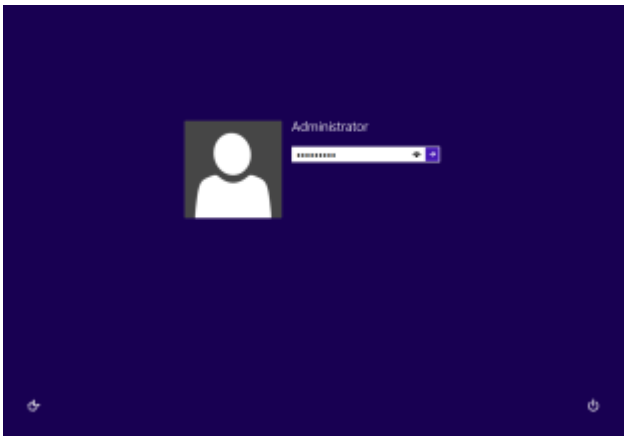
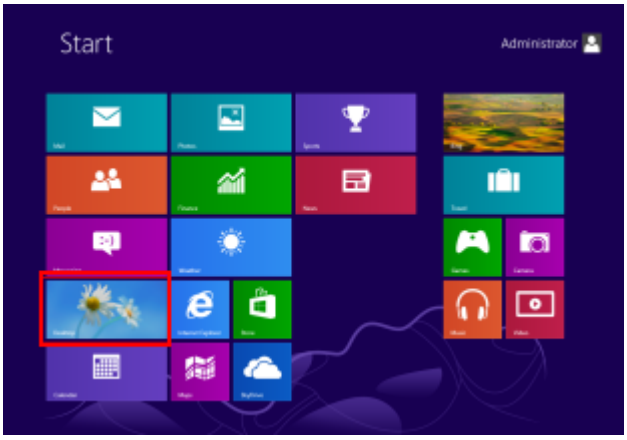
Schritt	Details
Schritt 9: Übernehmen Sie im Fenster **Processor Configuration** (Prozessorkonfiguration) die Standardwerte, und klicken Sie auf **Next** (Weiter).	
Schritt 10: Legen Sie im Fenster **Memory for the Virtual Machine** (Speicher für den virtuellen Computer) 2.048 MB als Speicher fest.	

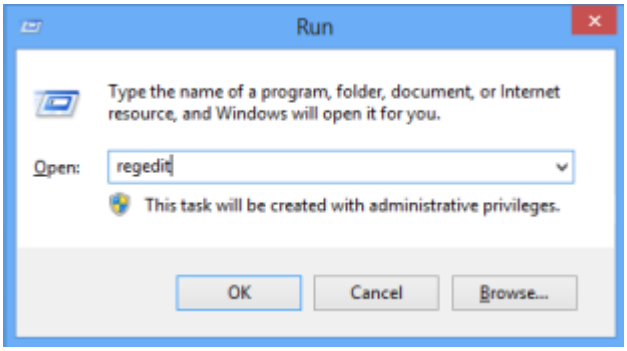
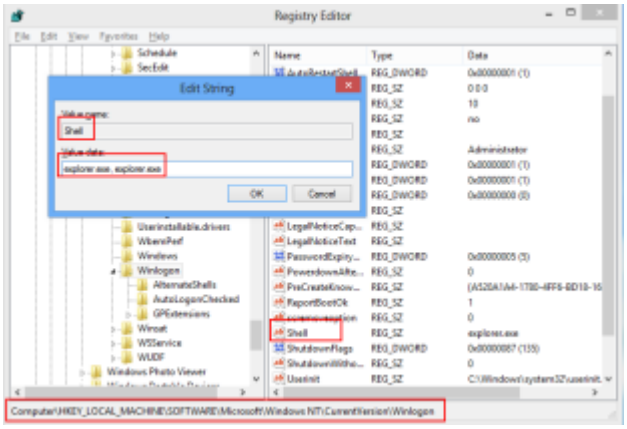
Schritt	Details
Schritt 11: Übernehmen Sie im Fenster **Network Type** (Netzwerktyp) die Standardauswahl.	
Schritt 12: Übernehmen Sie unter **Select I/O Controller Types** (Auswählen der I/O-Controller-Typen) die Standardauswahl.	

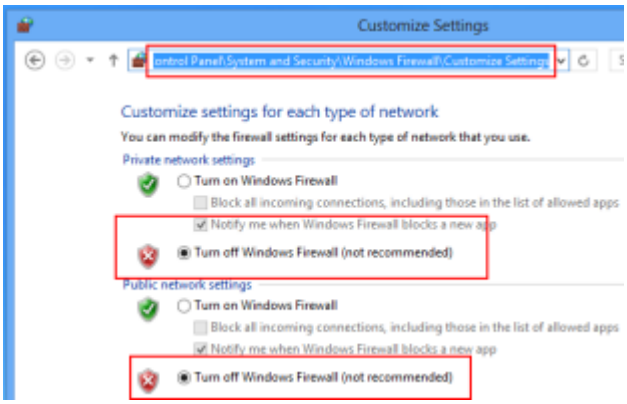
Schritt	Details
Schritt 13: Wählen Sie auf der Seite **Auswählen eines Datenträgertyps** die Option **IDE**, und klicken Sie auf **Next** (Weiter). SCSI-Datenträger sind mit McAfee Advanced Threat Defense nicht kompatibel.	
Schritt 14: Wählen Sie im Fenster **Auswählen eines Datenträgers** die Option **Create a new virtual disk** (Neuen virtuellen Datenträger erstellen), und klicken Sie auf **Next** (Weiter).	

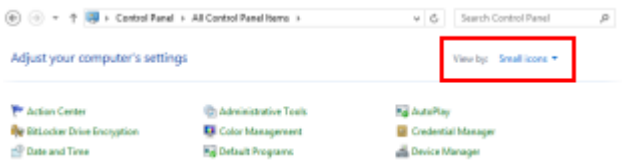
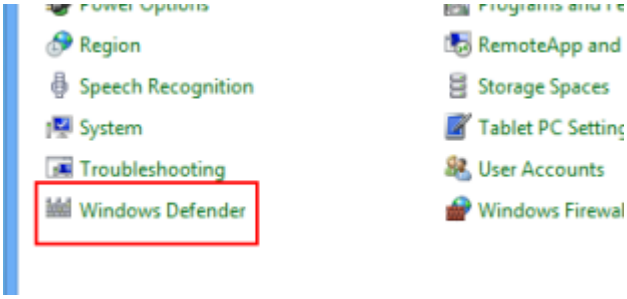
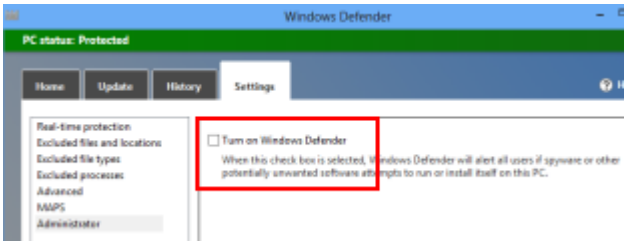
Schritt	Details
Schritt 15: Geben Sie die Details im Fenster **Angeben der Speicherkapazität** an, und klicken Sie auf **Next** (Weiter).	• **Maximum disk size (GB)** (Maximale Datenträgergröße (GB)) – Für Windows 8 64 und 32 Bit beträgt die Datenträgergröße 30 GB. Geben Sie jedoch 24 GB ein, um eine optimale Leistung zu gewährleisten. • Wählen Sie **Allocate all disk space now** (Sämtlichen Speicherplatz jetzt zuweisen). • Wählen Sie **Store virtual disk as a single file** (Virtuellen Datenträger als einzelne Datei speichern). 
Schritt 16: Vergewissern Sie sich, dass im Fenster **Specify Disk file** (Datenträgerdatei angeben) standardmäßig "virtualMachineImage.vmdk" angezeigt wird, und klicken Sie auf **Next** (Weiter). Wenn Sie unter **Virtual Machine name** (Name des virtuellen Computers) einen anderen Namen angegeben haben, wird dieser hier angezeigt.	

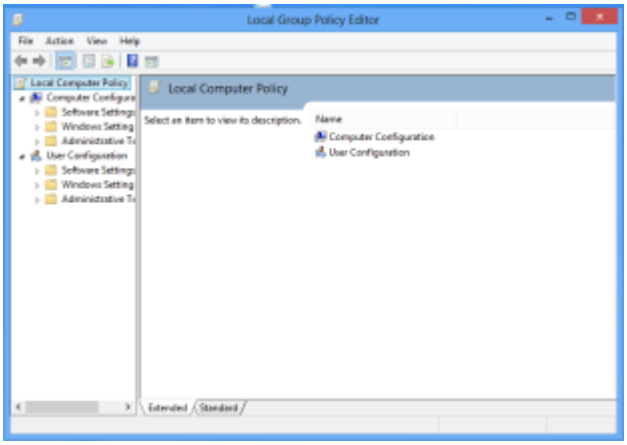
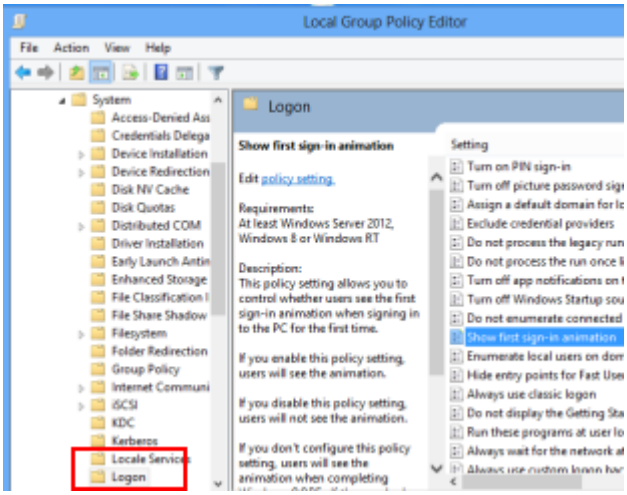
Schritt	Details
Schritt 17: Führen Sie folgende Schritte im Fenster **Ready to Create Virtual Machine** (Bereit zur Erstellung des virtuellen Computers) aus.	• **Power on this virtual machine after creation** (Diesen virtuellen Computer nach der Erstellung einschalten) – Wählen Sie diese Option. • Klicken Sie auf **Finish** (Fertig stellen). Dieser Schritt kann etwa 30 Minuten in Anspruch nehmen.  

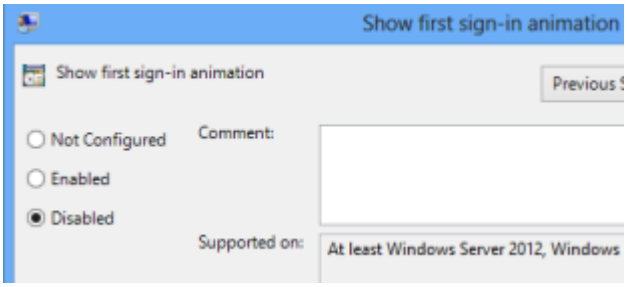
Schritt	Details
Schritt 18: Wenn das Popupfenster **Removable Devices** (Wechselgeräte) angezeigt wird, wählen Sie **Do not show this hint again** (Diesen Hinweis nicht mehr anzeigen), und klicken Sie auf **OK**.	Die Installation von Windows beginnt. Dies kann etwa 15 Minuten dauern. 
Schritt 19: Melden Sie sich mit den folgenden Anmeldeinformationen beim virtualMachineImage an: • Administrator • cr@cker42	
Schritt 20: Die VM wird standardmäßig im Modus "Metro UI" angezeigt. Klicken Sie auf die Kachel "Desktop", um in den Desktop-Modus zu wechseln.	

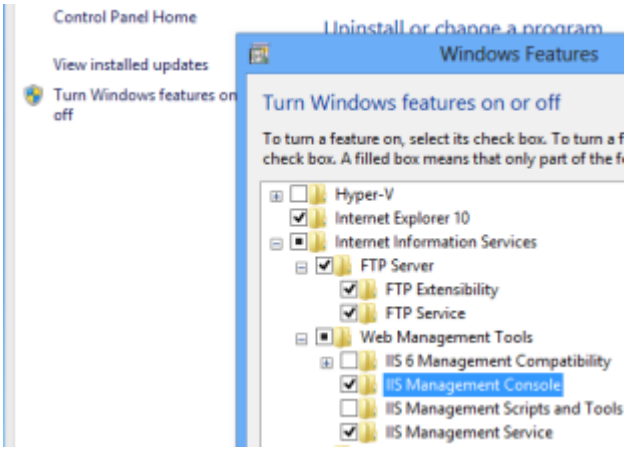
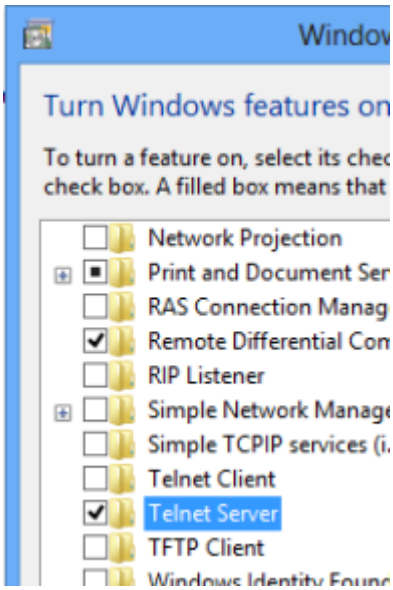
Schritt	Details
Schritt 21: Richten Sie Windows 8 so ein, dass beim Start der Desktop-Modus anstelle des Standardmodus "Metro UI" verwendet wird.	1 Drücken Sie gleichzeitig die Windows- und die R-Taste, um das Dialogfeld **Ausführen** zu öffnen. 2 Geben Sie im Dialogfeld **Ausführen** den Befehl `regedit` ein, und drücken Sie die Eingabetaste.  Der **Registrierungs-Editor** wird geöffnet. 3 Wählen Sie **HKEY_LOCAL_MACHINE** | **SOFTWARE** | **Microsoft** | **Windows NT** | **CurrentVersion** | **Winlogon** , und doppelklicken Sie anschließend auf **Shell**. 4 Ändern Sie den **Wert** vom Standardwert `explorer.exe` in `explorer.exe, explorer.exe`, und klicken Sie auf **OK**. 

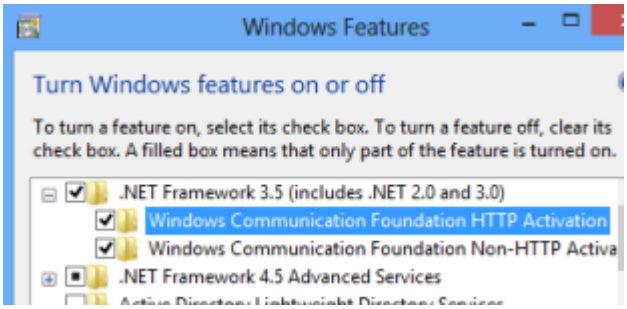
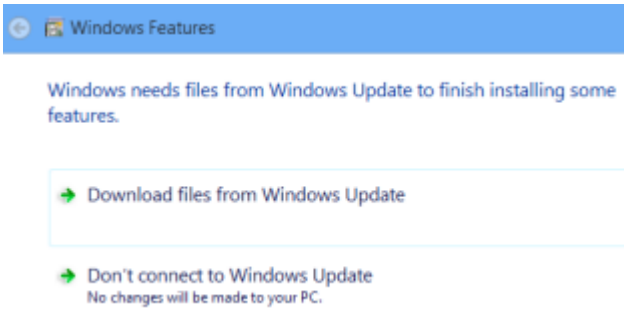
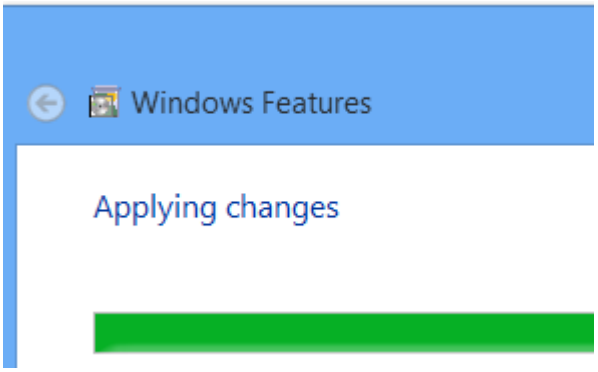
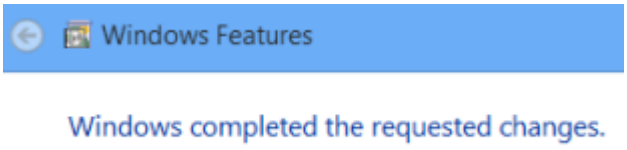
Schritt	Details
Schritt 22: Deaktivieren Sie auf der VM die Windows-Firewall.	1 Drücken Sie gleichzeitig die Windows- und die X-Taste, und wählen Sie dann **Systemsteuerung** | **System und Sicherheit** | **Windows-Firewall** | **Windows-Firewall ein- oder ausschalten**. 2 Wählen Sie **Windows-Firewall deaktivieren (nicht empfohlen)** für sowohl **Standorteinstellungen für das Heim- oder Arbeitsplatznetzwerk (privat)** als auch **Standorteinstellungen für das öffentliche Netzwerk**, und klicken Sie anschließend auf **OK**. 

Schritt	Details
Schritt 23: Deaktivieren Sie Windows Defender.	1 Öffnen Sie die Systemsteuerung, und wählen Sie aus dem Dropdown-Menü **Anzeigen nach** die Option **Kleine Symbole** aus.  2 Klicken Sie auf **Windows Defender**.  3 Wählen Sie in **Windows Defender Einstellungen** | **Administratoren** , und deaktivieren Sie **Windows Defender aktivieren**. Klicken Sie anschließend auf **Änderungen speichern**.  4 Schließen Sie das Windows Defender-Meldungsfeld. 

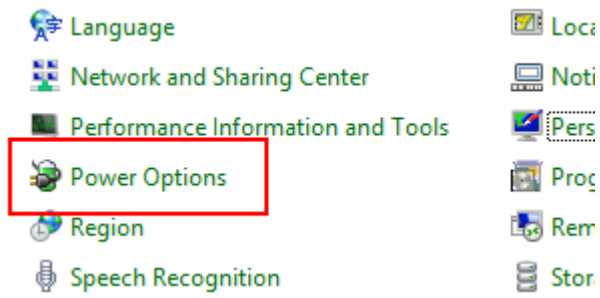
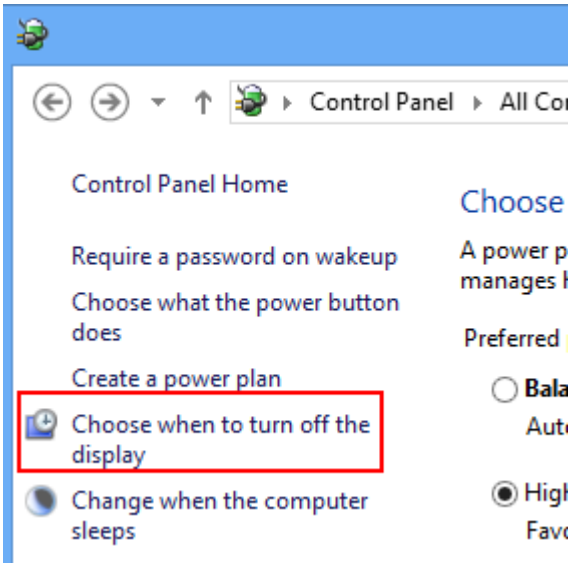
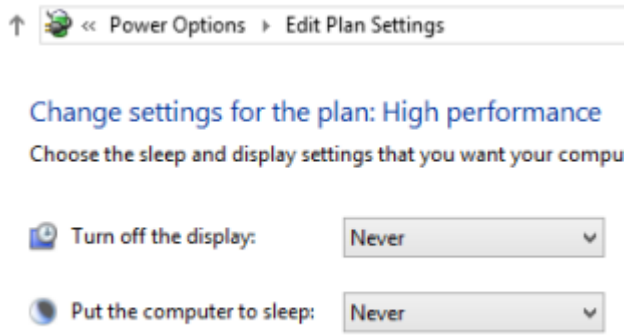
Schritt	Details
Schritt 24: Deaktivieren Sie die Animation zur ersten Anmeldung.	1 Drücken Sie gleichzeitig die Windows- und die R-Taste, um das Dialogfeld **Ausführen** zu öffnen. 2 Geben Sie im Dialogfeld **Ausführen** den Befehl `gpedit.msc` ein, und drücken Sie die Eingabetaste. Der **Editor für lokale Gruppenrichtlinien** wird geöffnet.  3 Wählen Sie **Computerkonfiguration** | **Administrative Vorlagen** | **System** | **Anmelden** , und öffnen Sie dann **Show first sign-in animation** (Animation zur ersten Anmeldung anzeigen).  4 Wählen Sie **Deaktiviert**, und klicken Sie anschließend auf **OK**.

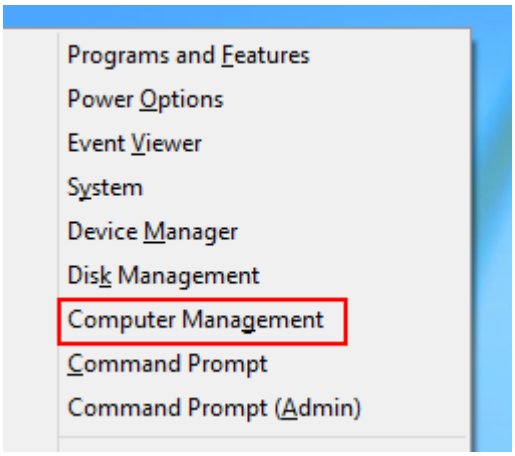
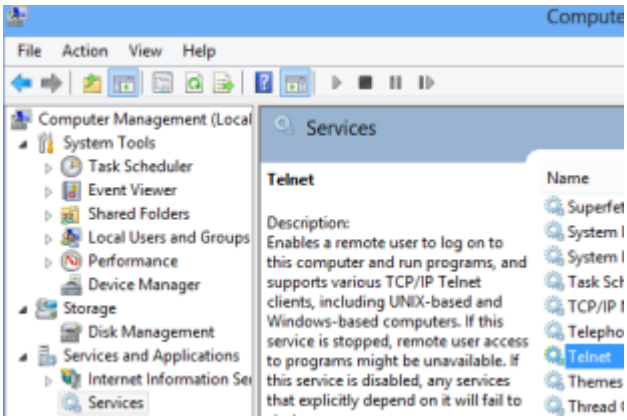
Schritt	Details
	

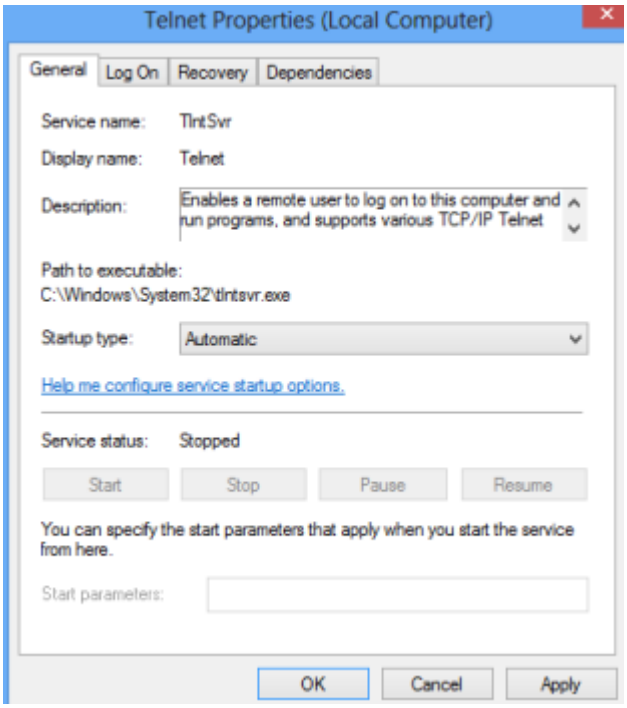
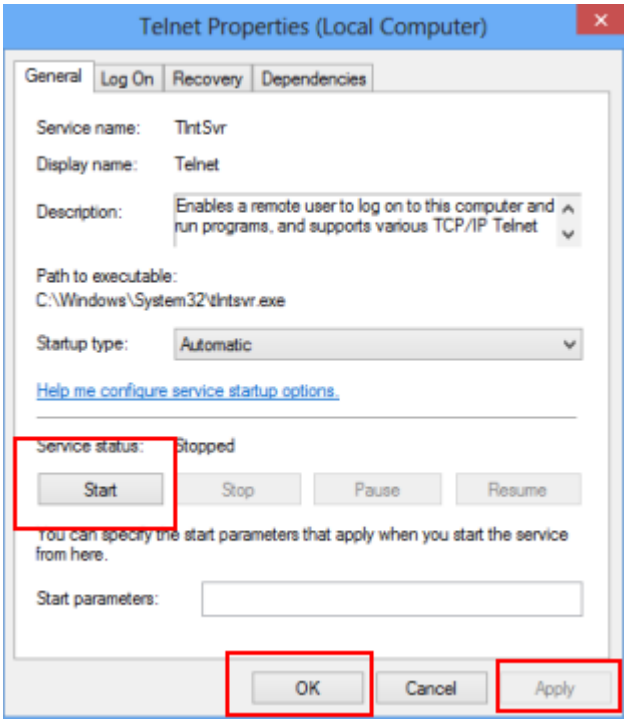
Schritt	Details
Schritt 25: Drücken Sie gleichzeitig die Windows- und die X-Taste, und wählen Sie dann **Systemsteuerung** | **Programme** | **Programme und Funktionen** | **Windows-Funktionen ein- oder ausschalten** , und führen Sie folgende Schritte aus.	**1** Wählen Sie **Internetinformationsdienste** | **FTP-Server** und **FTP-Erweiterbarkeit**. **2** Wählen Sie **Internetinformationsdienste** | **Webverwaltungstools** sowie **IIS-Verwaltungskonsole** und **IIS-Webverwaltungsdienst**.  **3** Wählen Sie **Telnet-Server**.  **4** Wählen Sie **.NET Framework 3.5 (einschließlich .NET 2.0 und 3.0)** und anschließend die Optionen **Nicht-HTTP-Aktivierung von Windows Communication Foundation** (HTTP-Aktivierung von Windows Communication Foundation) und **Windows Communication Foundation Non-HTTP Activation** (Nicht-HTTP-Aktivierung von Windows Communication Foundation).

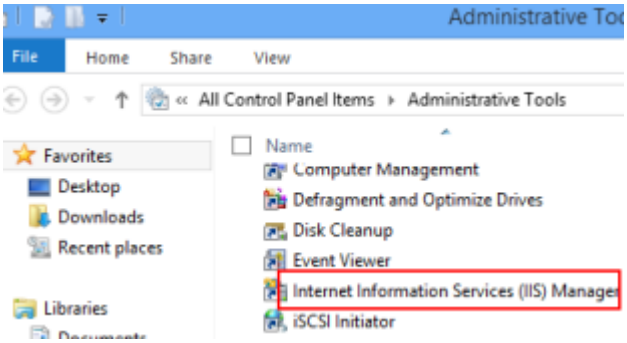
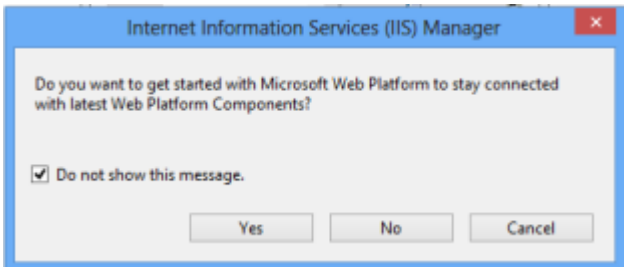
Schritt	Details
	 **5** Klicken Sie auf **OK**. **6** Sollte die folgende Meldung angezeigt werden, wählen Sie **Dateien von Windows Update herunterladen**.  Dieser Vorgang kann etwa 5 Minuten in Anspruch nehmen.  Eine Bestätigungsmeldung wird angezeigt, sobald der Vorgang abgeschlossen ist. 

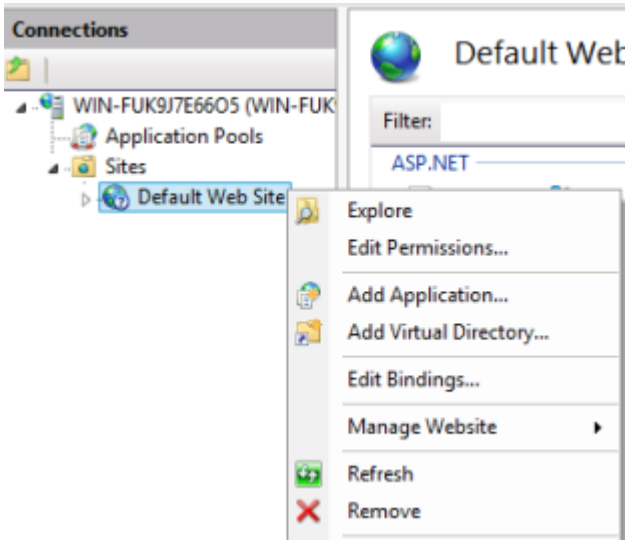
Schritt	Details

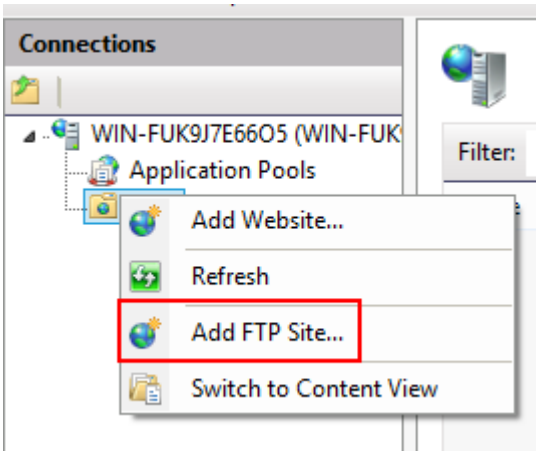
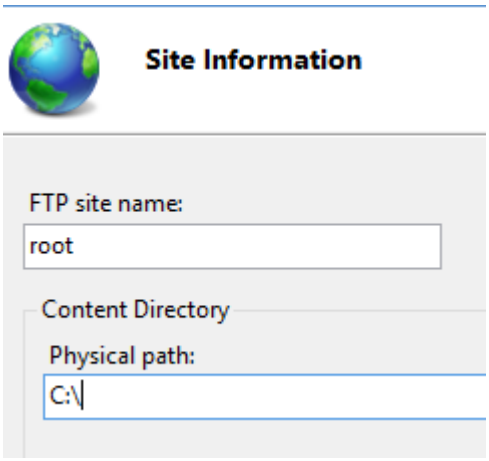
Schritt	Details
Schritt 26: Bearbeiten Sie die Energieoptionen.	1 Öffnen Sie die Systemsteuerung, und wählen Sie aus dem Dropdown-Menü **Anzeigen nach** die Option **Kleine Symbole** aus. 2 Klicken Sie auf **Energieoptionen**.  3 Klicken Sie auf **Zeitpunkt für das Ausschalten des Bildschirms auswählen**.  4 Wählen Sie sowohl für **Bildschirm ausschalten** als auch für **Energiesparmodus nach:** die Option **Nie** aus, und klicken Sie auf **Änderungen speichern**. 

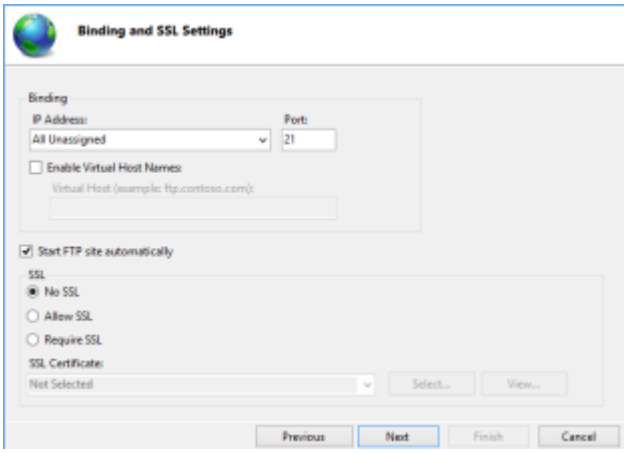
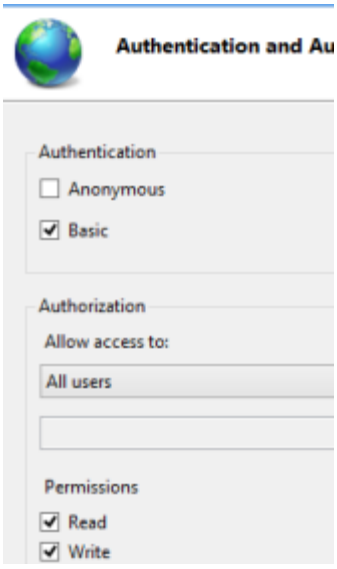
Schritt	Details
Schritt 27: Drücken Sie gleichzeitig die Windows- und die X-Taste, und wählen Sie dann **Computerverwaltung**	**Dienste und Anwendungen**	**Dienste**. Doppelklicken Sie anschließend auf **Telnet**.	 

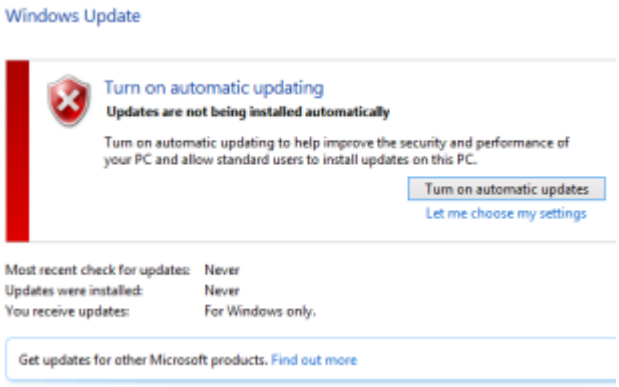
Schritt	Details
Schritt 28: Wählen Sie im Dialogfeld "Eigenschaften von Telnet (Lokaler Computer)" aus der Liste **Starttyp** die Option **Automatisch** aus. Wählen Sie dann **Übernehmen** | **Start** | **OK**.	 

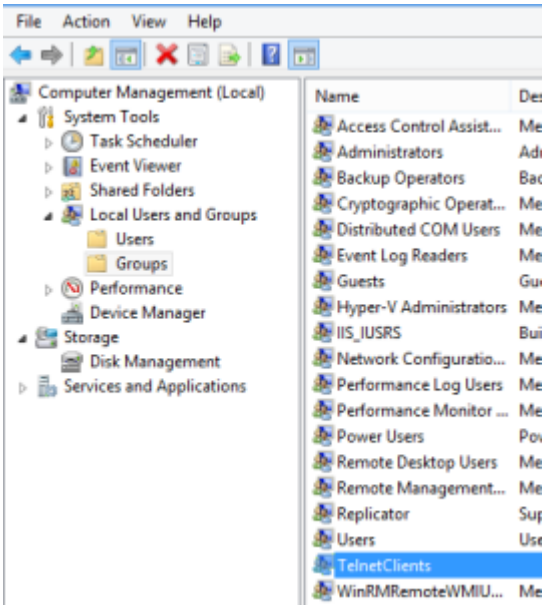
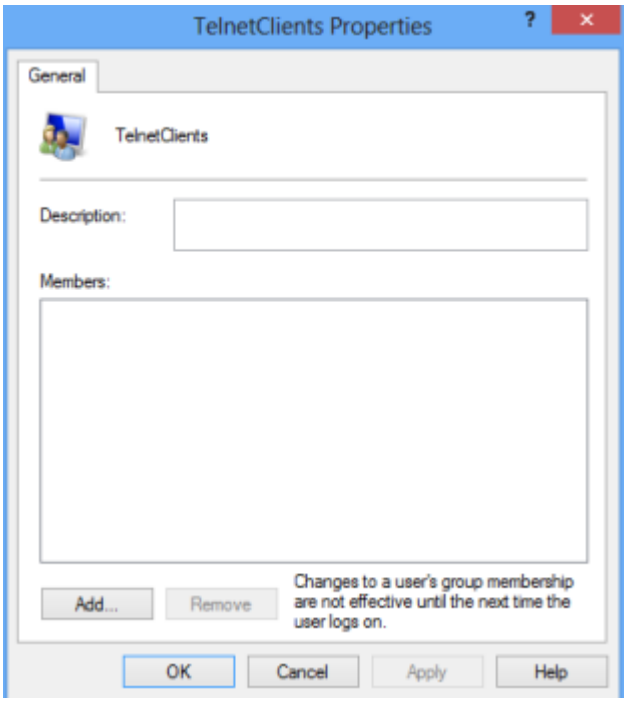
Schritt	Details
Schritt 29: Aktivieren Sie FTP unter Windows 8.	1 Drücken Sie gleichzeitig die Windows- und die X-Taste, und wählen Sie dann **Systemsteuerung** | **System und Sicherheit** | **Verwaltung**.  2 Doppelklicken Sie auf **Internetinformationsdienste-Manager**, und erweitern Sie die Baumstruktur unter **Hostname**. 3 Sollte folgendes Meldungsfeld angezeigt werden, wählen Sie **Do not show this message** (Diese Meldung nicht anzeigen), und klicken Sie auf **Abbrechen**. 4 Wählen Sie **Sites**  , klicken Sie mit der rechten Maustaste auf **Standardwebsite**, und wählen Sie anschließend **Entfernen**. Bestätigen Sie den Vorgang, indem Sie auf **Ja** klicken.

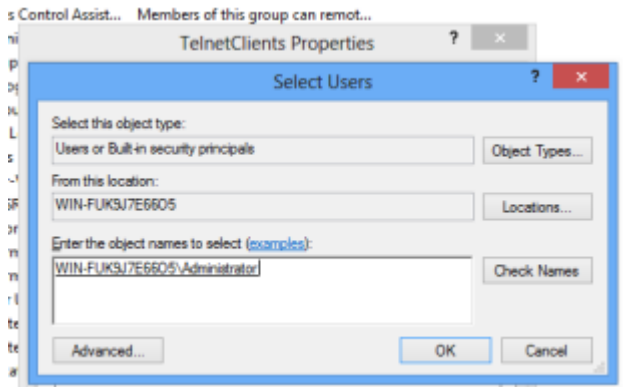
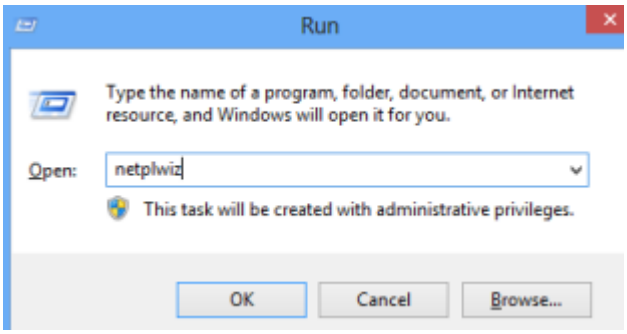
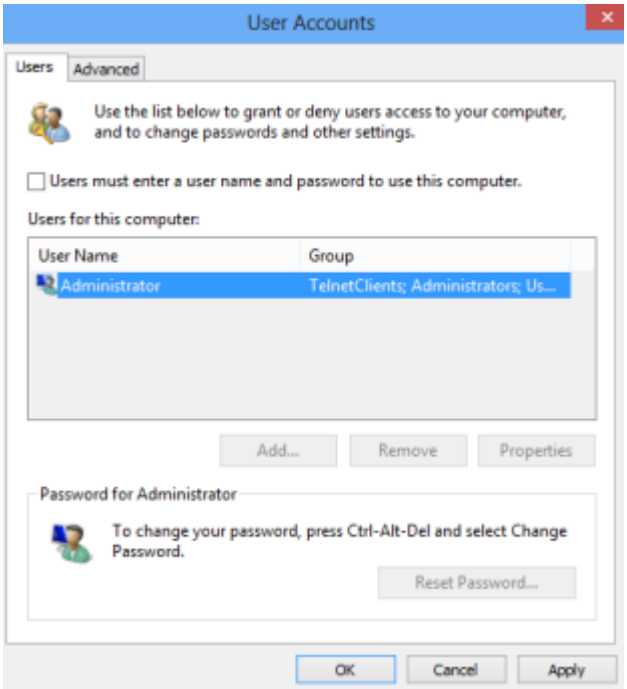
Schritt	Details
	

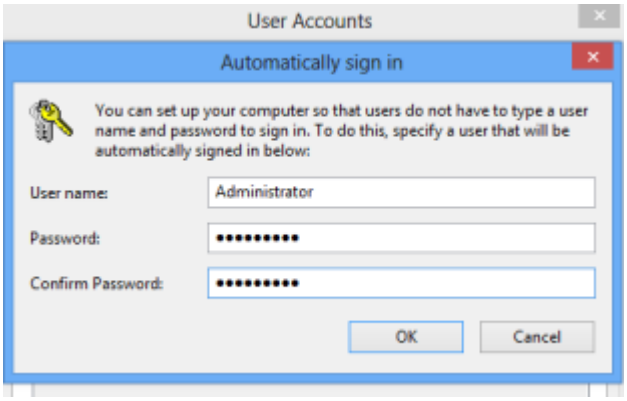
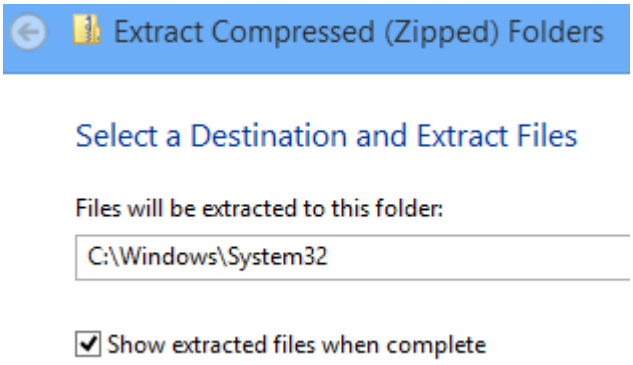
Schritt	Details
	5 Klicken Sie mit der rechten Maustaste auf **Sites**, und wählen Sie **FTP-Site hinzufügen**. Führen Sie dann folgende Schritte aus.  **a** Geben Sie unter **FTP-Sitename** `root` ein. **b** **Physischer Pfad: C:\.** **c** Klicken Sie auf **Weiter**.  **6** Wählen Sie unter **Bindungen und SSL-Einstellungen** die Option **Kein SSL**. Akzeptieren Sie bei allen anderen Feldern die Standardwerte, und klicken Sie auf **Weiter**.

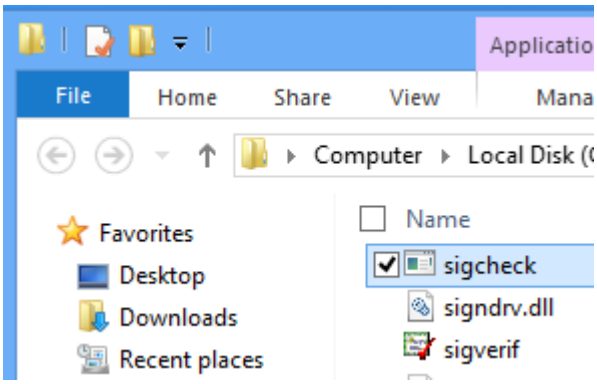
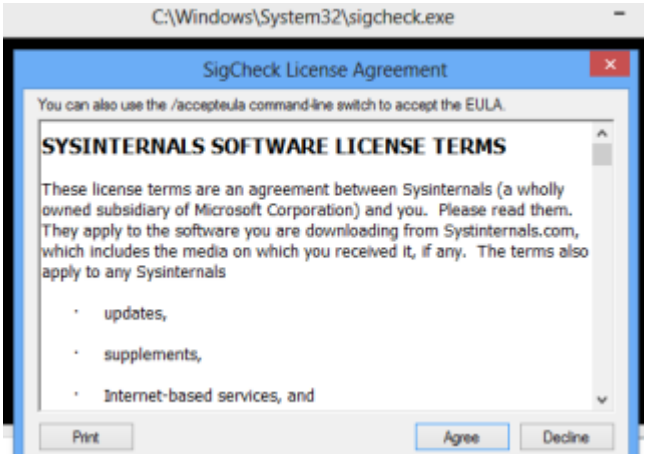
Schritt	Details
	 **7** Führen Sie unter **Authentifizierungs- und Autorisierungsinformationen** folgende Schritte aus. **a** Wählen Sie **Standard**. **b** Unter **Zugriff zulassen für** wählen Sie **Alle Benutzer**. **c** Wählen Sie unter **Berechtigungen** sowohl **Lesen** als auch **Schreiben**, und klicken Sie anschließend auf **Fertig stellen**. **d** Schließen Sie das Fenster **Internetinformationsdienste-Manager**. 

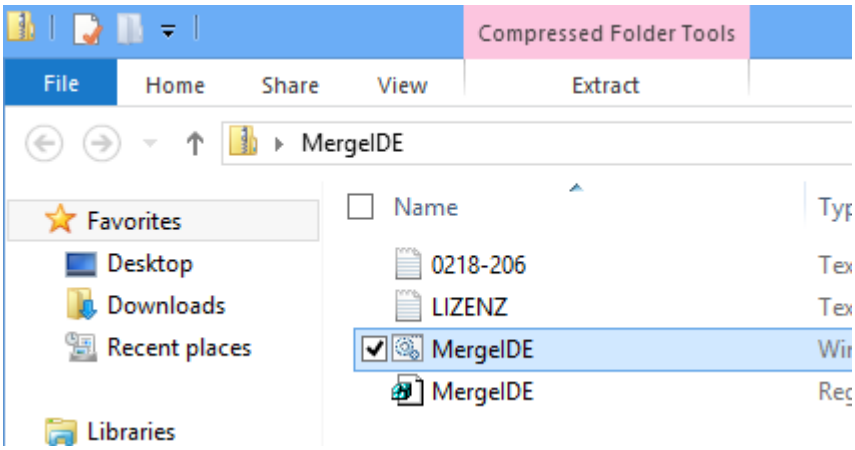
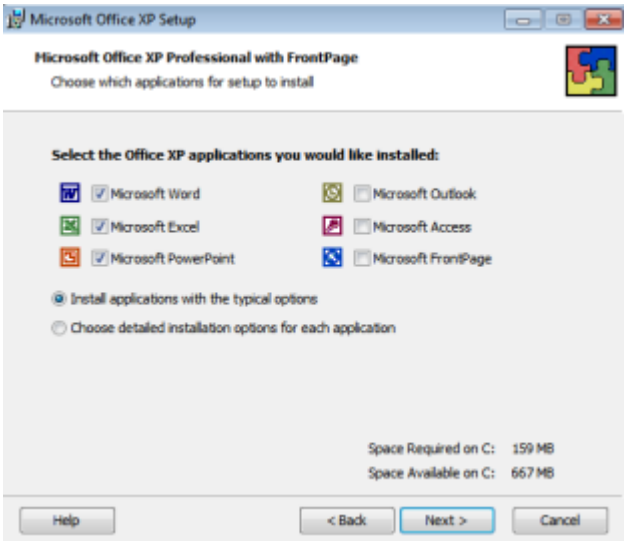
Schritt	Details
Schritt 30: Deaktivieren Sie die automatische Aktualisierung für Windows.	1 Drücken Sie gleichzeitig die Windows- und die X-Taste, und wählen Sie dann **Systemsteuerung** | **Windows-Update** | **Ändern**. 2 Wählen Sie **Nie nach Updates suchen (nicht empfohlen)**, und klicken Sie auf **OK**. 

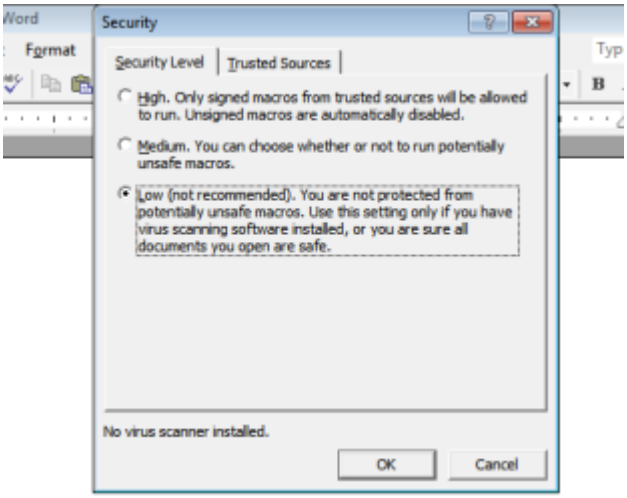
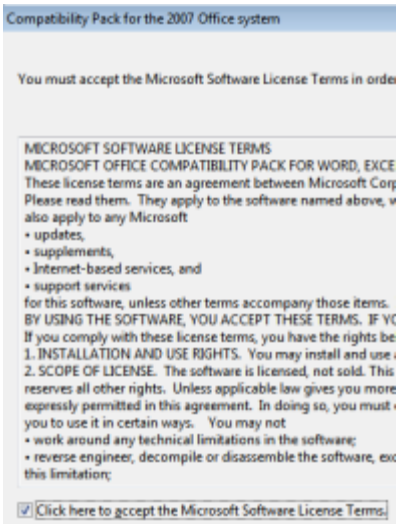
Schritt	Details
Schritt 31: Führen Sie die folgenden Schritte aus: 1 Öffnen Sie die Systemsteuerung, und wählen Sie aus dem Dropdown-Menü **Anzeigen nach** die Option **Kleine Symbole** aus. 2 Wählen Sie **Administratortools** | **Computerverwaltung** , und führen Sie die Schritte in der nächsten Spalte aus.	1 Wählen Sie **Computerverwaltung (Lokal)** | **System** | **Lokale Benutzer und Gruppen** | **Gruppen** aus.  2 Doppelklicken Sie auf **TelnetClients**.  3 Klicken Sie auf **Hinzufügen**, und geben Sie `Administrator` ein. 4 Klicken Sie auf **Namen überprüfen** und anschließend auf **OK**.

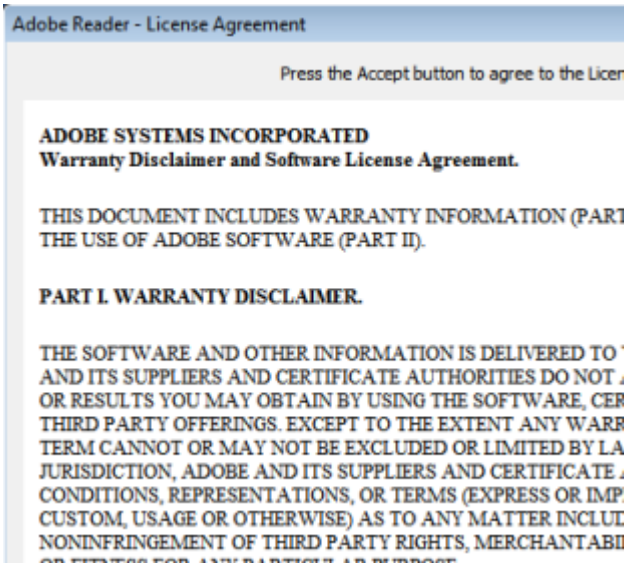
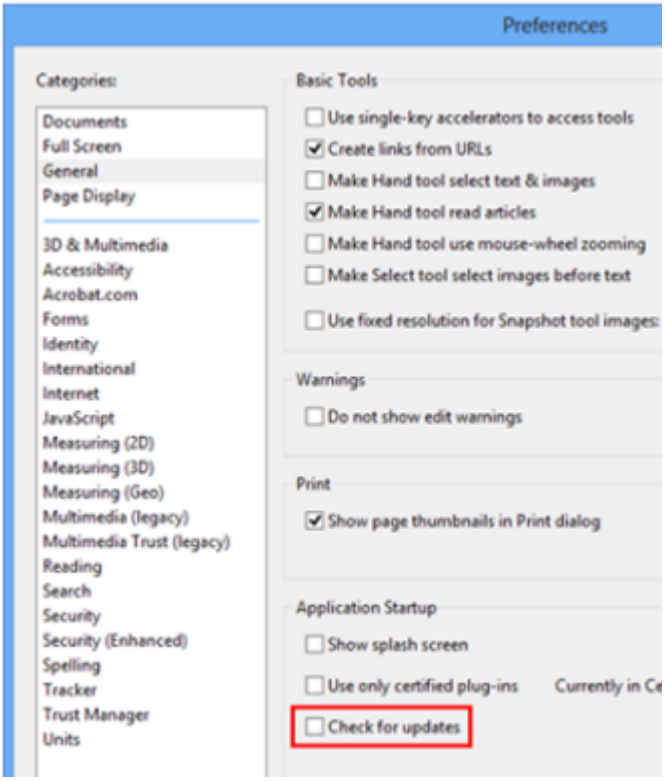
Schritt	Details
	
Schritt 32: Drücken Sie gleichzeitig die Windows- und die R-Taste, um das Dialogfeld **Ausführen** zu öffnen. Geben Sie anschließend `netplwiz` ein, und klicken Sie auf **OK**.	
Schritt 33: Deaktivieren Sie im Fenster **Benutzerkonten** die Option **Benutzer müssen Benutzernamen und Kennwort eingeben**, und klicken Sie auf **Übernehmen**.	

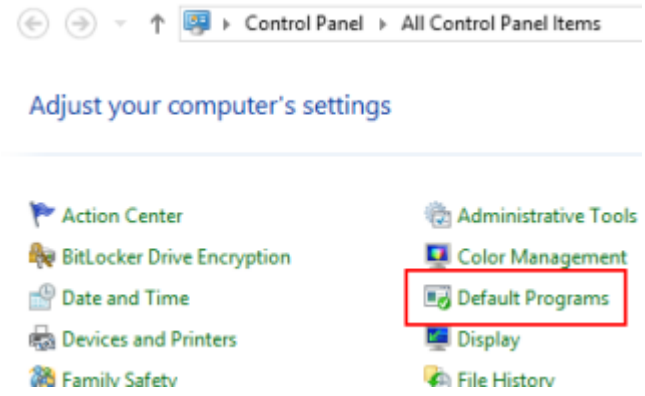
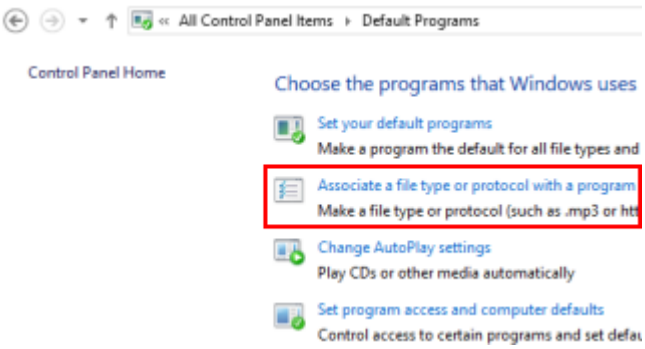
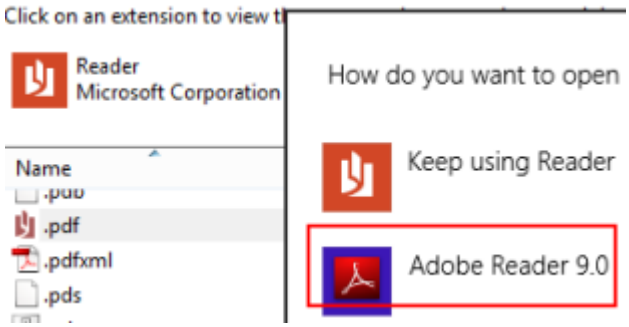
Schritt	Details
Schritt 34: Führen Sie im Popupfenster **Automatische Anmeldung** die folgenden Schritte aus, und klicken Sie dann auf **OK**.	• **Benutzername** – Geben Sie `Administrator` ein. • **Kennwort** – Geben Sie `cr@cker42` ein. • **Kennwort bestätigen** – Geben Sie `cr@cker42` erneut ein. 
Schritt 35: Laden Sie Sigcheck von der Seite http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx auf Ihren Computer (den nativen Host) herunter.	Auf der von Ihnen erstellten VM ist die Windows-Firewall deaktiviert. Außerdem ist kein Virenschutz installiert. Daher wird empfohlen, die Programme und Komponenten zuerst auf den nativen Host herunterzuladen und dann auf die VM in VMware Workstation zu kopieren.
Schritt 36: Extrahieren Sie "sigcheck.zip" an folgendem Speicherort: `C:\WINDOWS\system32`.	

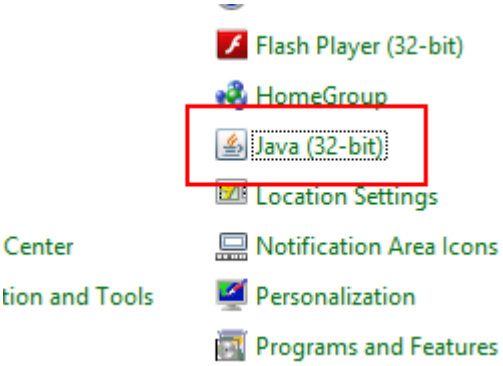
Schritt	Details
Schritt 37: Navigieren Sie in Windows Explorer zu C:\WINDOWS\system32, und doppelklicken Sie auf **sigcheck.exe**.	
Schritt 38: Klicken Sie im **Sigcheck License Agreement** (Sigcheck-Lizenzvertrag) auf **Agree** (Ich stimme zu). Nach dem Klicken auf **Agree** (Ich stimme zu) wird keine Bestätigungsmeldung angezeigt.	
Schritt 39: Laden Sie die ZIP-Datei "MergeIDE.zip" von der Seite https://www.virtualbox.org/attachment/wiki/Migrate_Windows/MergeIDE.zip auf den nativen Computer herunter, und kopieren Sie sie auf die VM.	

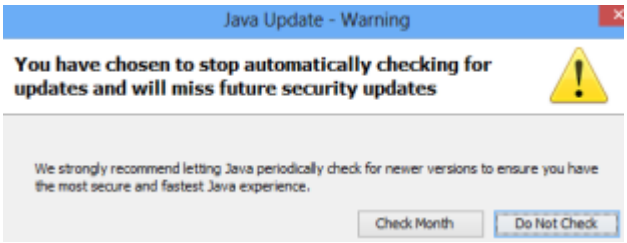
Schritt	Details
Schritt 40: Extrahieren Sie MergeIDE.zip, und führen Sie die MergeIDE-Batchdatei auf der VM aus.	 • Klicken Sie in der Warnmeldung auf **Ausführen**, wenn Sie dazu aufgefordert werden. • Schließen Sie Windows Explorer.
Schritt 41: Um Microsoft Word-, Excel- und PowerPoint-Dateien zu analysieren, installieren Sie Microsoft Office 2003 auf dem virtuellen Computer.	

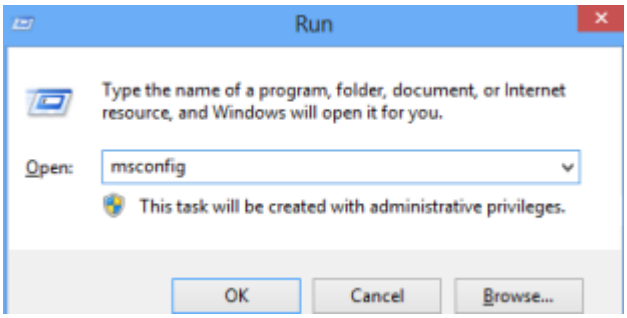
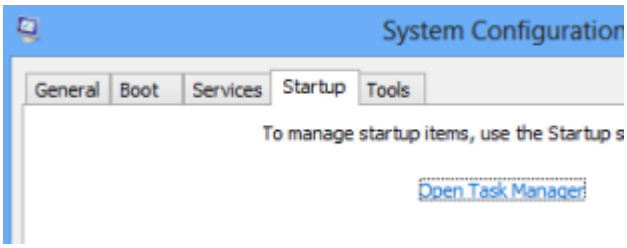
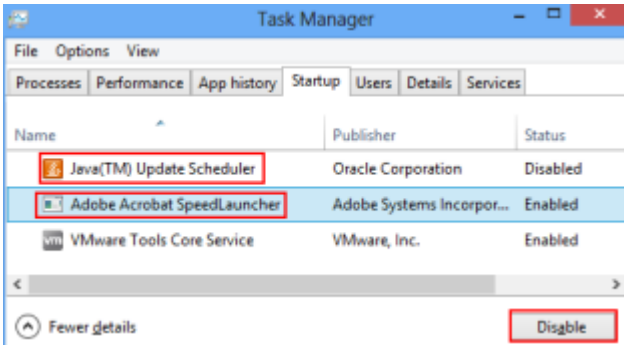
Schritt	Details
Schritt 42: Senken Sie die Sicherheitsstufe, um Makros für Office-Anwendungen auszuführen.	• Öffnen Sie Microsoft Word 2003, und wählen Sie **Extras** | **Makro** | **Sicherheit** und dann **Niedrig**, und klicken Sie auf **OK**.  • Setzen Sie genauso die Makrosicherheit für Microsoft Excel und PowerPoint herab.
Schritt 43: Sie benötigen das Compatibility Pack, um Microsoft Office-Dateien öffnen zu können, die mit einer neueren Version von Microsoft Office erstellt wurden. Beispiel: Zum Öffnen einer DOCX-Datei mit Office 2003 muss das entsprechende Compatibility Pack installiert sein. Rufen Sie http://www.microsoft.com/en-us/download/details.aspx?id=3 auf, und laden Sie das erforderliche Microsoft Office Compatibility Pack für Word-, Excel- und PowerPoint-Dateiformate herunter. Installieren Sie es anschließend auf dem virtuellen Computer.	Aktivieren Sie im Dialogfeld **Compatibility Pack für 2007 Office System** die Option **Klicken Sie hier, um den Microsoft-Software-Lizenzbedingungen zuzustimmen**, und klicken Sie auf **Weiter**. 

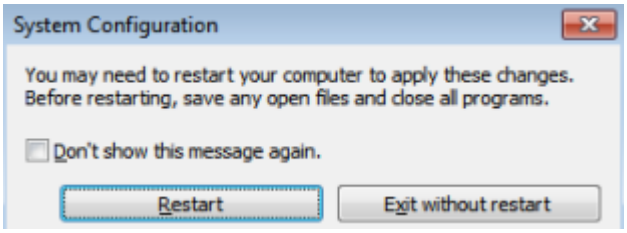
Schritt	Details
Schritt 44: Um PDF-Dateien zu analysieren, laden Sie Adobe Reader auf den nativen Host herunter, und kopieren Sie ihn auf die VM. In diesem Beispiel wird Adobe Reader 9.0 verwendet.	1 Installieren Sie Adobe Reader 9.0 auf der VM. 2 Öffnen Sie Adobe Reader, und klicken Sie auf **Akzeptieren**.  3 Wählen Sie in Adobe Reader **Bearbeiten** | **Voreinstellungen** | **Allgemein** , und deaktivieren Sie **Nach Updates suchen**. 

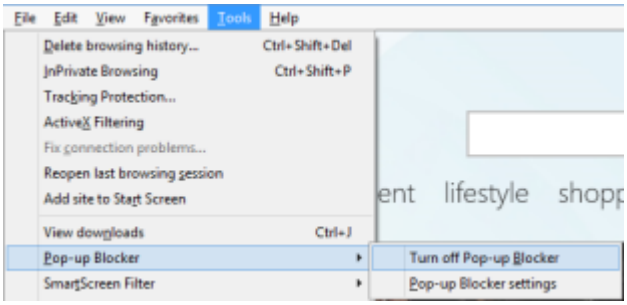
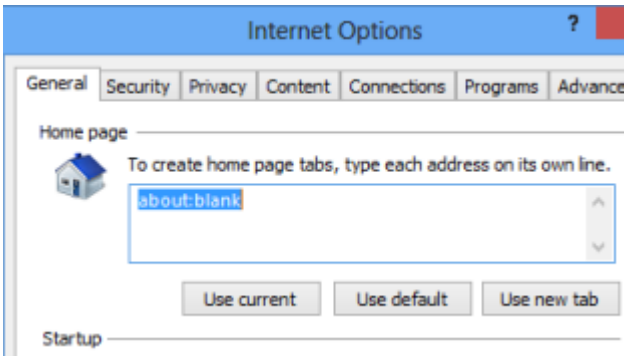
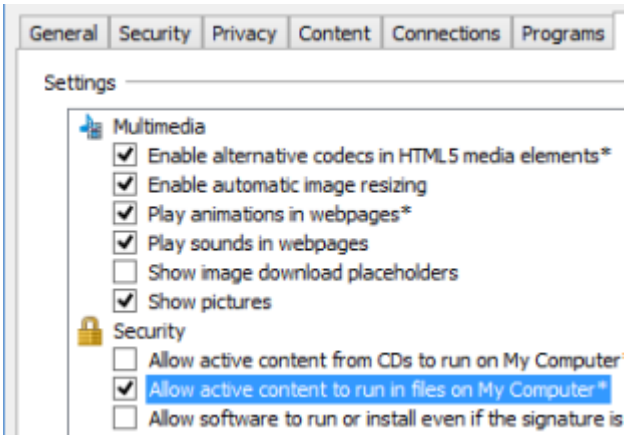
Schritt	Details
Schritt 45: Legen Sie Adobe Reader 9 als Standardanwendung zum Öffnen von PDF-Dateien fest.	1 Wählen Sie in der **Systemsteuerung** (Symbolansicht) **Standardprogramme** aus.  2 Wählen Sie **Dateityp oder Protokoll einem Programm zuordnen** aus.  3 Suchen Sie nach **.pdf**, und doppelklicken Sie darauf. Wählen Sie Adobe Reader 9.0 als Standard-PDF-Reader aus. 

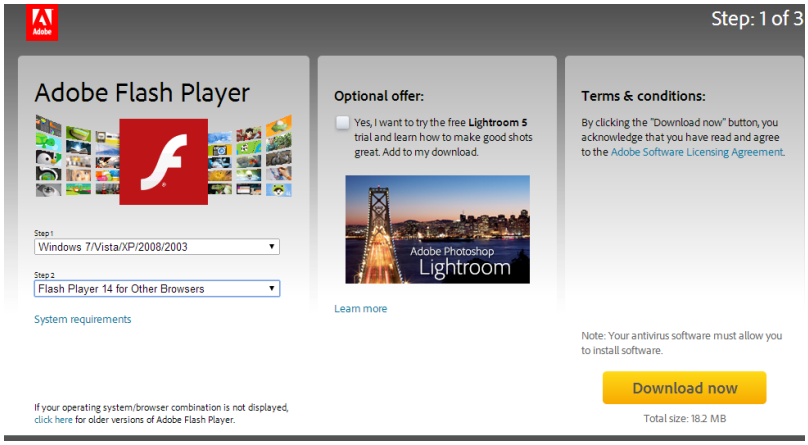
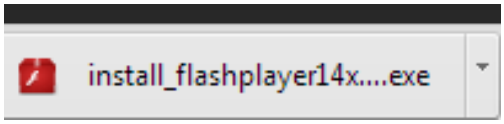
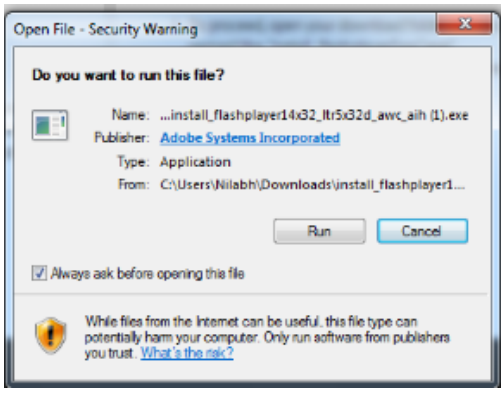
Schritt	Details
Schritt 46: Laden Sie zum Analysieren von JAR-Dateien Java Runtime Environment herunter, und installieren Sie die Anwendung. In diesem Beispiel wird Java 7 Update 25 verwendet.	
Schritt 47: Öffnen Sie Java in der Systemsteuerung.	
Schritt 48: Deaktivieren Sie auf der Registerkarte **Update** die Option **Automatisch nach Updates suchen**.	

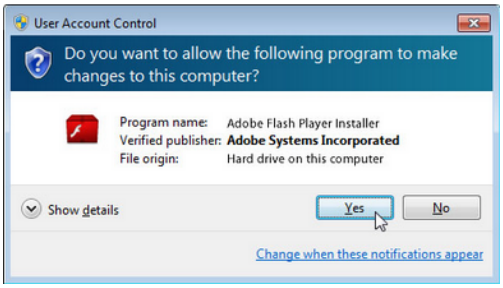
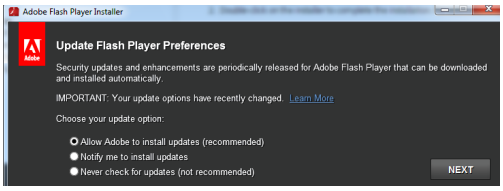
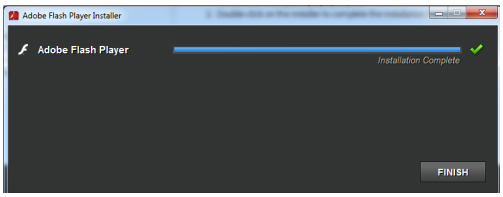
Schritt	Details
Schritt 49: Wählen Sie im Dialogfeld "Java-Update – Warnung" die Option **Nicht überprüfen**, und klicken Sie dann in der Java-Systemsteuerung auf **OK**.	

Schritt	Details
Schritt 50: Deaktivieren Sie *jusched* und *reader_sl*.	1 Drücken Sie gleichzeitig die Windows- und die R-Taste, um das Dialogfeld **Ausführen** zu öffnen. Geben Sie im Windows-Dialogfeld "Ausführen" `msconfig` ein, und klicken Sie auf **OK**.  2 Navigieren Sie im **Systemkonfigurationsprogramm** zur Registerkarte **Start**.  3 Klicken Sie auf **Task-Manager öffnen**. 4 Wenn *Java(TM) Update Scheduler* (jusched) aufgeführt ist, wählen Sie es aus, und klicken Sie auf **Deaktivieren**. 5 Wenn *Adobe Acrobat SpeedLauncher* (reader_sl) aufgeführt ist, wählen Sie es aus, und klicken Sie auf **Deaktivieren**.  6 Aktivieren Sie im Dialogfeld **Systemkonfiguration** das Kontrollkästchen **Diese Meldung nicht mehr anzeigen**, und klicken Sie auf **Neu starten**.

Schritt	Details
	

Schritt	Details
Schritt 51: Öffnen Sie den Standard-Browser, und richten Sie ihn für Malware-Analysen ein. In diesem Beispiel wird Internet Explorer verwendet.	1 Stellen Sie sicher, dass der Popupblocker ausgeschaltet ist. Wählen Sie in Internet Explorer **Extras** | **Popupblocker** | **Popupblocker ausschalten.**  2 Wählen Sie **Extras** | **Internetoptionen** , und geben Sie unter **Startseite** `about:blank` ein.  3 Wechseln Sie zur Registerkarte **Erweitert**, und suchen Sie **Sicherheit**. 4 Wählen Sie **Ausführung aktiver Inhalte in Dateien auf dem lokalen Computer zulassen** aus.  5 Klicken Sie auf **OK**.

Schritt	Details
Schritt 52: Um eine Flash-Datei (SWF) dynamisch zu analysieren, installieren Sie die erforderliche Version von Adobe Flash. In diesem Beispiel wird Flash Player 14 verwendet.	1 Rufen Sie http://get.adobe.com/flashplayer/otherversions/ auf. 2 Wählen Sie gemäß Ihren Anforderungen ein Betriebssystem und eine Flash Player-Version in den Dropdown-Menüs **Schritt 1** und **Schritt 2** aus (siehe unten). 3 Klicken Sie auf **Jetzt herunterladen**.  4 Doppelklicken Sie in der unteren Ecke Ihres Bildschirms auf die Installationsdatei für Adobe Flash Player **(install_flashplayer xxx.exe)**.  5 Klicken Sie im Dialogfeld **Sicherheitswarnung** auf **Ausführen**.  6 Klicken Sie im Dialogfeld **Benutzerkontensteuerung** auf **Ja**.

Schritt	Details
	 **7** Wählen Sie Ihre Aktualisierungsoption, und klicken Sie auf **WEITER**.  **8** Klicken Sie auf **FERTIGSTELLEN**, um die Adobe Flash Player-Installation abzuschließen. 
Schritt 53: Fahren Sie die VM herunter.	
Schritt 54: Navigieren Sie zu dem Speicherort, den Sie in Schritt 8 angegeben haben, um die VMDK-Datei mit dem Namen `virtualMachineImage-flat.vmdk` aufzurufen.	Falls erforderlich, können Sie die VMDK-Datei in "Windows 8 x64-flat.vmdk" oder "Windows 8 x32-flat.vmdk" umbenennen.

Importieren einer VMDK-Datei in McAfee Advanced Threat Defense

Bevor Sie beginnen

- Sie haben die VMDK-Datei parat.
- Das Betriebssystem der VM ist aktiv, und auf ihr sind alle erforderlichen Anwendungen wie Microsoft Office-Anwendungen, Adobe PDF Reader usw. installiert.
- Im Dateinamen der VMDK-Datei sind keine Leerzeichen enthalten. Wenn er Leerzeichen enthält, schlägt die Konvertierung der Image-Datei fehl.

Zum Erstellen einer Analyse-VM müssen Sie zunächst die zugehörige VMDK-Datei in McAfee Advanced Threat Defense importieren. Standardmäßig müssen Sie zum Importieren der VMDK-Datei SFTP benutzen. Um FTP verwenden zu können, müssen Sie es mit dem CLI-Befehl `set ftp` aktivieren. Siehe set ftp auf Seite 364.

Im Allgemeinen ist eine FTP-Übertragung schneller als SFTP, sie bietet jedoch weniger Sicherheit. Wenn sich Ihre Advanced Threat Defense Appliance in einem unsicheren Netzwerk befindet (z. B. in einem externen Netzwerk), empfiehlt McAfee die Verwendung von SFTP.

Vorgehensweise

1. Öffnen Sie einen FTP-Client.

   Beispielsweise eignen sich WinSCP oder FileZilla.

2. Stellen Sie mithilfe der folgenden Anmeldeinformationen eine Verbindung zum FTP-Server auf McAfee Advanced Threat Defense her.
   - Host: IP-Adresse von McAfee Advanced Threat Defense
   - Benutzername: atdadmin
   - Kennwort: atdadmin
   - Port: die Portnummer für das Protokoll, das Sie verwenden möchten
3. Laden Sie die VMDK-Datei vom lokalen Computer in McAfee Advanced Threat Defense hoch.

Konvertieren der VMDK-Datei in eine Image-Datei

Bevor Sie beginnen

- Sie haben die VMDK-Datei auf McAfee Advanced Threat Defense hochgeladen.
- Sie verfügen über Administratorberechtigungen in McAfee Advanced Threat Defense.

Vorgehensweise

1. Wählen Sie in der McAfee Advanced Threat Defense-Web-Anwendung **Verwalten** | **Image Management (Image-Verwaltung)**.
2. Klicken Sie auf der Seite **Image Management** (Image-Verwaltung) auf die VMDK-Datei, die Sie über das Dropdown-Menü **VMDK Image** (VMDK-Image) importiert haben.

3 Benennen Sie die Image-Datei.

> Der Name muss aus 1 bis 20 Zeichen bestehen und darf keine Leerzeichen enthalten. Enthält der Name der Image-Datei ein Leerzeichen, schlägt die Konvertierung in die Image-Datei fehl.

Für die Malware-Analyse benötigen Sie möglicherweise mehrere Analyse-VMs, die auf demselben Betriebssystem, aber mit verschiedenen Anwendungen laufen. Beispiel: Sie benötigen möglicherweise eine Analyse-VM unter Windows 7 SP1 mit Internet Explorer 10 und eine weitere Analyse-VM unter Windows 7 SP1 mit Internet Explorer 11. Wenn Sie mehrere Analyse-VMs mit demselben Betriebssystem erstellen möchten, ist die Angabe eines **Image-Namens** obligatorisch. Möchten Sie nur eine Analyse-VM für ein bestimmtes Betriebssystem erstellen, ist die Angabe des **Image-Namens** optional. Wenn Sie keinen Namen angeben, wird der Image-Datei ein Standardname zugewiesen, mit dem Sie u. a. die Protokolle anzeigen und VM-Profile erstellen können.

Im Folgenden werden die Standardnamen für Image-Dateien aufgeführt:

- **winXPsp2**: bezieht sich auf Microsoft Windows XP (32 Bit) Service Pack 2
- **winXPsp3**: bezieht sich auf Microsoft Windows XP (32 Bit) Service Pack 3
- **win7sp1**: bezieht sich auf Microsoft Windows 7 (32 Bit) Service Pack 1
- **win7x64sp1**: bezieht sich auf Microsoft Windows 7 (64 Bit) Service Pack 1
- **win2k3sp1**bezieht sich auf Microsoft Windows Server 2003 (32 Bit) Service Pack 1
- **win2k3sp2**bezieht sich auf Microsoft Windows Server 2003 (32 Bit) Service Pack 2
- **win2k8sp1**bezieht sich auf Microsoft Windows Server 2008 R2 Service Pack 1
- **win8p0x32**: bezieht sich auf Microsoft Windows 8 (32 Bit)
- **win8p0x64**: bezieht sich auf Microsoft Windows 8 (64 Bit)

Der von Ihnen angegebene Name wird an den Standardnamen angehängt. Sie geben beispielsweise als *Image-Namen* die Bezeichnung **with_PDF** an, und das Betriebssystem ist Windows Server 2003 (32 Bit) Service Pack 1. Die Image-Datei erhält dann den Namen *win2k3sp1_with_PDF*.

> Wenn Sie versuchen, mehrere Analyse-VMs mit demselben Betriebssystem zu erstellen, wird die Image-Datei jedes Mal mit der Standardbezeichnung für das Betriebssystem benannt. Daher wird diese Image-Datei jedes Mal überschrieben, anstatt eine neue Analyse-VM mit demselben Betriebssystem zu erstellen. Aus diesem Grund ist es obligatorisch, bei der Erstellung mehrerer Analyse-VMs mit demselben Betriebssystem einen **Image-Namen** anzugeben.

4 Wählen Sie das entsprechende Betriebssystem aus dem Dropdown-Menü **Operating System** (Betriebssystem) aus.

5 Klicken Sie auf **Konvertieren**.

Die benötigte Zeit für die Konvertierung hängt von der Größe der VMDK-Datei ab. Für eine 15 GB große Datei benötigt ATD-3000 etwa fünf Minuten.

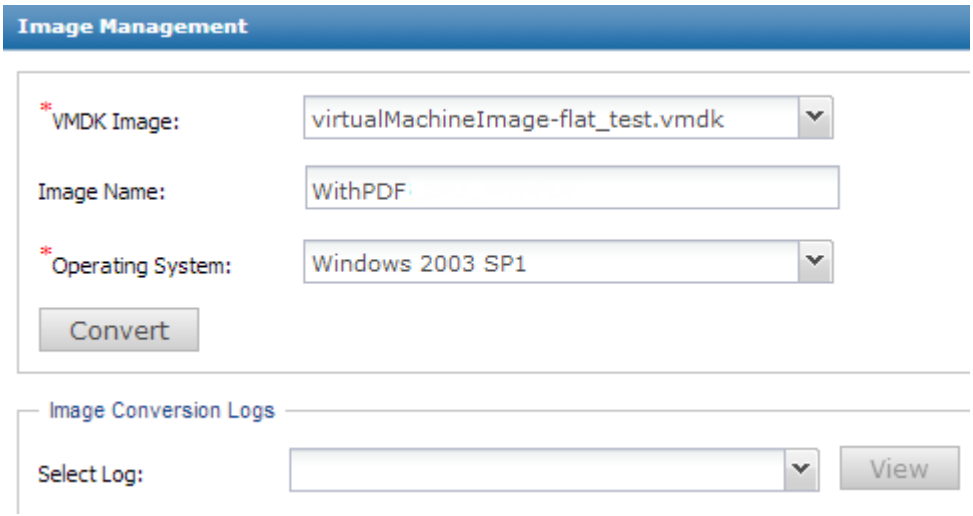


Abbildung 5-2 Konvertierung einer VMDK- in eine Image-Datei

Nach Abschluss der Konvertierung wird eine Meldung angezeigt.

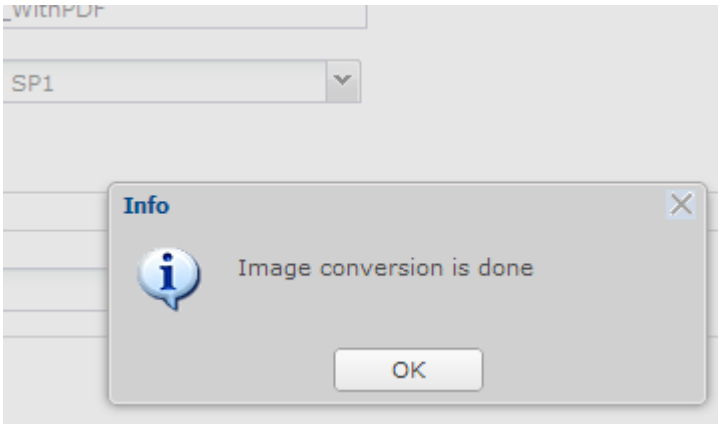


Abbildung 5-3 Bestätigungsmeldung

6 Um die Protokolle für die Image-Konvertierung anzuzeigen, wählen Sie den Image-Namen aus der Liste **Select Log** (Protokoll auswählen) aus, und klicken Sie auf **Anzeigen**.

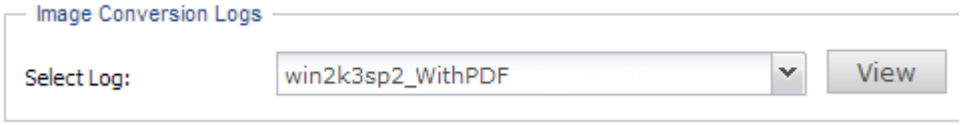


Abbildung 5-4 Auswählen der Image-Datei zum Anzeigen der Protokolle

Wenn kein **Image-Name** angegeben wurde, wird der Image-Datei ein auf dem Betriebssystem basierender Standardname zugewiesen. Wurde ein **Image-Name** angegeben, wird der angegebene Name an den Standardnamen angehängt.

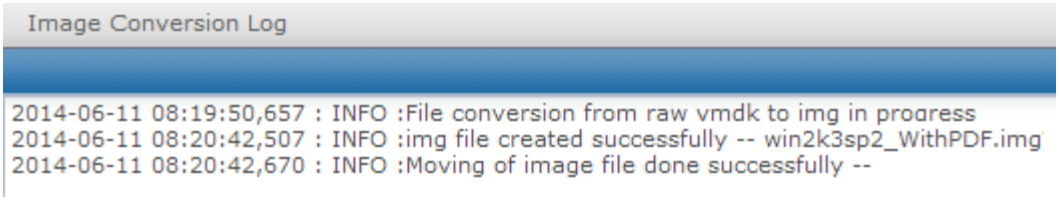

Image Conversion Log
2014-06-11 08:19:50,657 : INFO :File conversion from raw vmdk to img in progress
2014-06-11 08:20:42,507 : INFO :img file created successfully -- win2k3sp2_WithPDF.img
2014-06-11 08:20:42,670 : INFO :Moving of image file done successfully --

Abbildung 5-5 Protokolleinträge zur Image-Konvertierung

Verwalten von VM-Profilen

Nach dem Konvertieren der importierten VMDK-Datei in eine Image-Datei erstellen Sie für diese Image-Datei ein VM-Profil.

Sie können dieses VM-Profil nicht mit einer anderen Image-Datei verknüpfen. Gleichfalls können bereits mit einem VM-Profil verknüpfte Image-Dateien nicht nachträglich geändert werden.

Die Image-Dateien enthalten das Betriebssystem und die Anwendungen für das VM-Profil. Sie können mit ihrer Hilfe die in McAfee Advanced Threat Defense hochgeladenen Images identifizieren und das jeweils zutreffende Image zur dynamischen Dateianalyse benutzen. Sie können auch die Anzahl der Lizenzen festlegen, die Sie für das Betriebssystem und die Anwendungen besitzen. McAfee Advanced Threat Defense berücksichtigt diese Informationen beim Erstellen übereinstimmender Analyse-VMs von einer Image-Datei.

Die VM-Profile können mittels McAfee Advanced Threat Defense-Web-Anwendung verwaltet werden.

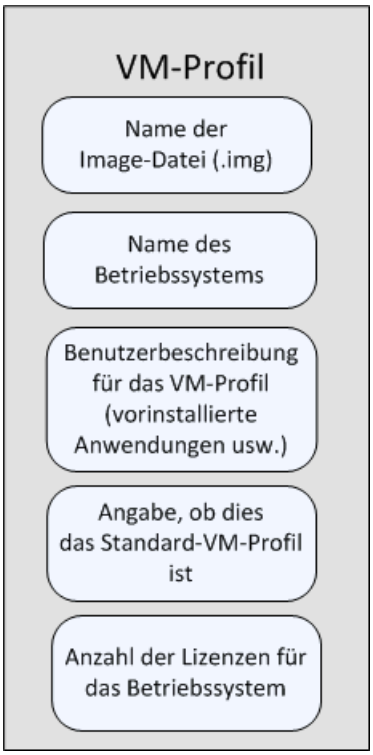

VM-Profil
Name der Image-Datei (.img)
Name des Betriebssystems
Benutzerbeschreibung für das VM-Profil (vorinstallierte Anwendungen usw.)
Angabe, ob dies das Standard-VM-Profil ist
Anzahl der Lizenzen für das Betriebssystem

Abbildung 5-6 Konfigurationen in einem VM-Profil

Anzeigen von VM-Profilen

Sie können die vorhandenen VM-Profile in der McAfee Advanced Threat Defense-Web-Anwendung anzeigen.

Vorgehensweise

1 Wählen Sie **Richtlinie** | **VM-Profil**.

Die verfügbaren VM-Profile werden aufgeführt.

Spaltenname	Beschreibung
Auswählen	Dient zum Bearbeiten oder Löschen des entsprechenden VM-Profils.
Name	Der von Ihnen zugewiesene Name des VM-Profils.
Licenses (Lizenzen)	Die Anzahl der Endbenutzerlizenzen, über die Sie für das entsprechende Betriebssystem und die Anwendungen verfügen. Dies ist einer der Faktoren, die die Anzahl der gleichzeitigen Analyse-VMs auf McAfee Advanced Threat Defense festlegen.
Default (Standard)	Zeigt an, ob es sich um ein Standard-VM-Profil handelt.
Size (Größe)	Die Größe der Image-Datei in MB.
Hash	Der MD5-Hash-Wert der Image-Datei.

2 Blenden Sie die überflüssigen Spalten aus.

a Bewegen Sie den Mauszeiger über die rechte Ecke einer Spaltenüberschrift, und klicken Sie auf den Dropdown-Pfeil.

b Wählen Sie **Columns** (Spalten).

c Wählen Sie nur die erforderlichen Spaltennamen aus der Liste.

Sie können auf eine Spaltenüberschrift klicken und sie an die gewünschte Position ziehen.

3 Zum Sortieren der Datensätze basierend auf einem bestimmten Spaltennamen klicken Sie auf die Spaltenüberschrift.

Sie können die Datensätze in auf- oder absteigender Reihenfolge sortieren. Alternativ können Sie den Mauszeiger über die rechte Ecke einer Spaltenüberschrift bewegen und auf den Dropdown-Pfeil klicken. Wählen Sie dann **Sort Ascending** (Aufsteigend sortieren) oder **Sort Descending** (Absteigend sortieren).

4 Zum Anzeigen aller Details eines bestimmten VM-Profils wählen Sie den Datensatz aus, und klicken Sie auf **View** (Anzeigen).

Erstellen von VM-Profilen

Nachdem Sie die VDMK-Datei in das Image-Format konvertiert haben, können Sie mit der VM-Erstellung beginnen und auch das entsprechende VM-Profil erstellen.

Jede Image-Datei, die Sie konvertiert haben, darf nur mit einem VM-Profil verknüpft sein. Das bedeutet, dass Sie für jedes zu erstellende VM-Profil eine nicht verwendete Image-Datei benötigen. Allerdings können Sie die Image-Dateien einer VMDK-Datei mehrfach konvertieren. Dadurch können Sie mehrere Image-Dateien aus einer VMDK-Datei erstellen.

Vorgehensweise

1 Wählen Sie **Richtlinie** | **VM-Profil** | **Neu.**.

Die Seite **VM-Profil** wird angezeigt.

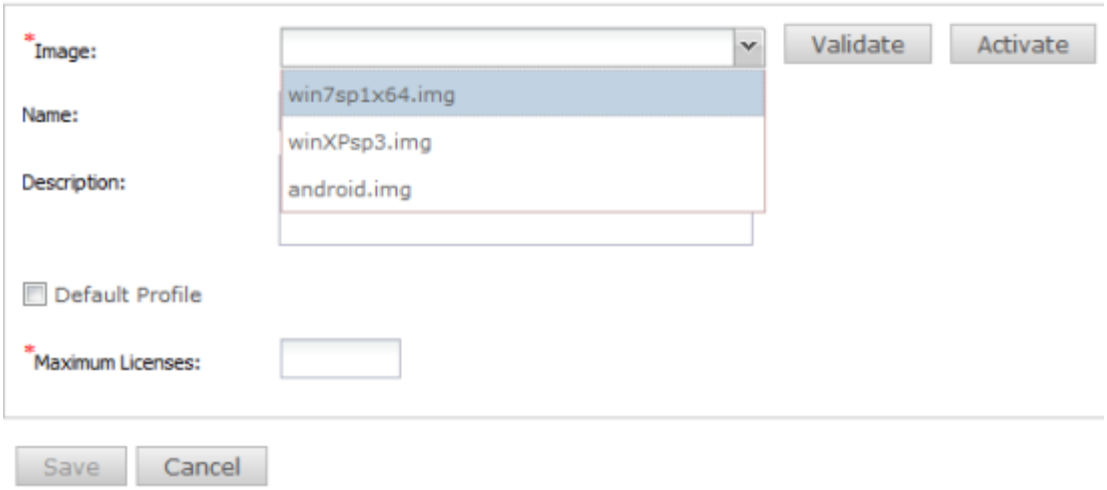


Abbildung 5-7 Auswählen der Image-Datei

2 Wählen Sie im Dropdown-Menü **Image** die Image-Datei aus, für die Sie das VM-Profil erstellen möchten.

3 Klicken Sie auf **Aktivieren**, um die VM von der ausgewählten Image-Datei zu erstellen.

- Wenn Sie auf **Aktivieren** klicken, wird die VM in einem Popupfenster geöffnet. Vergewissern Sie sich daher, dass der Popupblocker Ihres Browsers deaktiviert ist.
- Dies hat nichts mit der Windows-Aktivierung von Microsoft zu tun. Sie müssen erst die Windows-Aktivierung abschließen, bevor Sie die VMDK-Datei mithilfe von FTP oder SFTP in McAfee Advanced Threat Defense importieren können.

In einem Fortschrittsbalken wird die VM-Erstellung angezeigt.

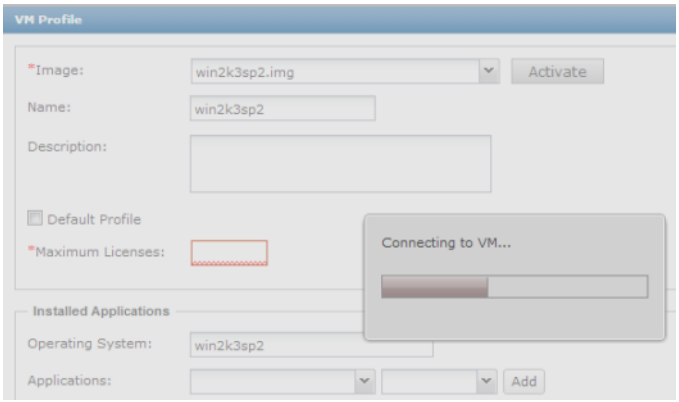


Abbildung 5-8 Fortschritt der VM-Erstellung

Abhängig von Ihren Browsereinstellungen werden Warnmeldungen vor dem Start der VM angezeigt.

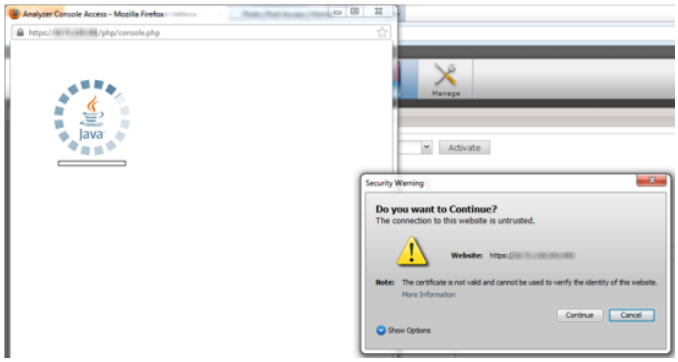


Abbildung 5-9 Warnmeldung

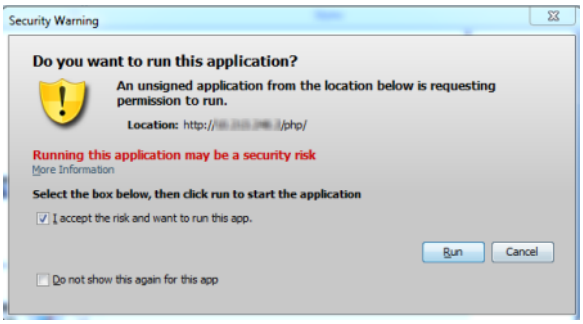

Security Warning
Do you want to run this application?
An unsigned application from the location below is requesting permission to run.
Location: http://
/php/
Running this application may be a security risk
More Information
Select the box below, then click run to start the application
I accept the risk and want to run this app.
Run
Cancel
Do not show this again for this app

Abbildung 5-10 Warnmeldung

Nachdem Sie die Warnmeldungen bestätigt haben, startet die VM.

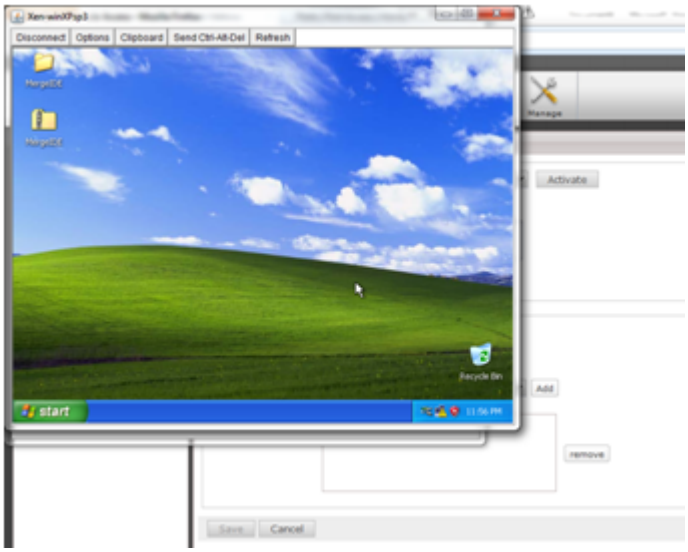


Abbildung 5-11 In einem Popupfenster angezeigte VM

4 Nachdem die VM hochgefahren ist, fahren Sie sie herunter, und schließen Sie das Popupfenster.

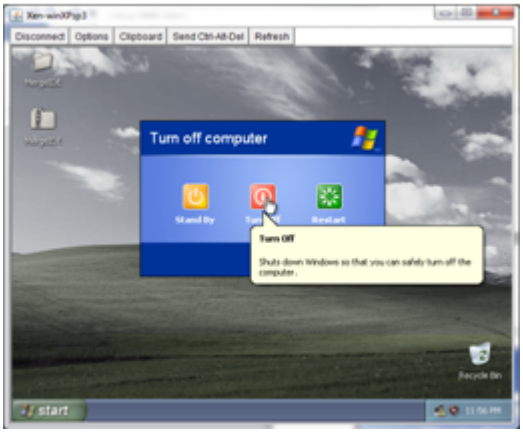


Abbildung 5-12 Herunterfahren der VM

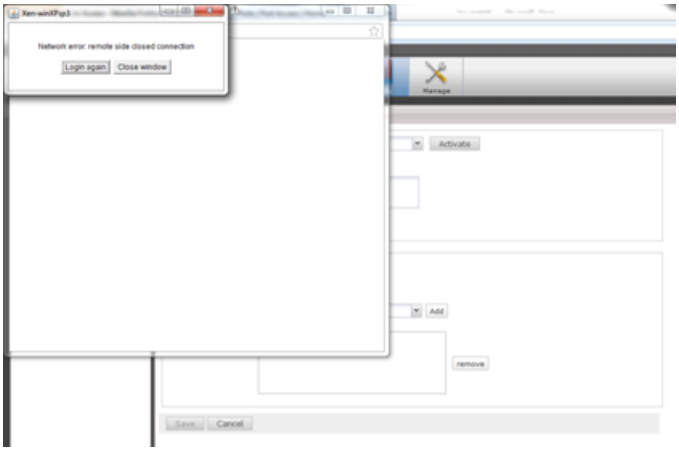


Abbildung 5-13 Schließen des Popupfensters

5 Klicken Sie auf **Überprüfen**.



Abbildung 5-14 Validieren der Image-Datei

McAfee Advanced Threat Defense stellt sicher, dass die VM an die Hardware der McAfee Advanced Threat Defense Appliance angepasst ist. Das Programm überprüft auch die Funktionstüchtigkeit der VM und die installierten Anwendungen, konfiguriert die Netzwerkdetails usw. Wenn die VM ordnungsgemäß funktioniert, war die Validierung erfolgreich.

Klicken Sie auf **Status überprüfen**, um das Image-Validierungsprotokoll anzuzeigen. Sie können die Erstellung des VM-Profils nur fortsetzen, wenn die Validierung erfolgreich war. Ist die Validierung fehlgeschlagen, finden Sie die Ursache im Validierungsprotokoll. Erstellen Sie anschließend eine neue VMDK mit den richtigen Einstellungen, und wiederholen Sie den Prozess der Analyse-VM-Erstellung.

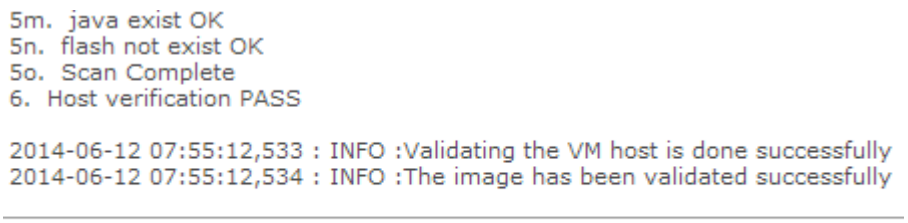

5m. java exist OK
5n. flash not exist OK
5o. Scan Complete
6. Host verification PASS
2014-06-12 07:55:12,533 : INFO :Validating the VM host is done successfully
2014-06-12 07:55:12,534 : INFO :The image has been validated successfully

Abbildung 5-15 Image-Validierungsprotokoll

6 Erstellen Sie das VM-Profil für die erstellte VM, indem Sie die entsprechenden Informationen in die jeweiligen Felder eingeben.

Tabelle 5-4 Optionsbeschreibungen

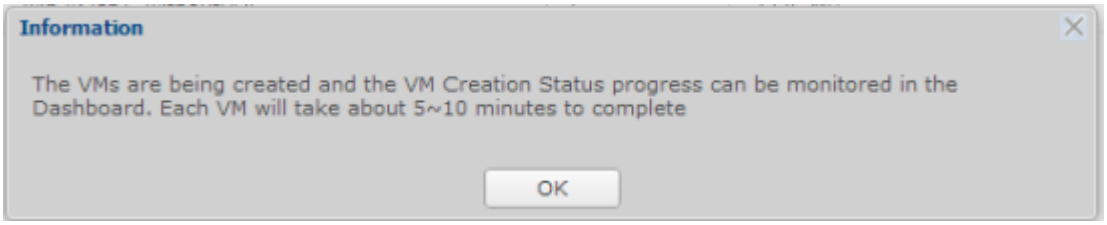
Optionsname	Beschreibung
Name	Der Name der Image-Datei wird automatisch als Name für das VM-Profil angezeigt. Sie können ihn nicht ändern.
Beschreibung	Geben Sie optional eine ausführliche Beschreibung des VM-Profils an.

Tabelle 5-4 Optionsbeschreibungen *(Fortsetzung)*

Optionsname	Beschreibung
Default Profile (Standardprofil)	Beim ersten Mal müssen Sie das VM-Profil auswählen, um es als Standard festzulegen. Danach können Sie es auswählen oder ignorieren. McAfee Advanced Threat Defense verwendet diese VM für die dynamische Analyse, wenn für eine Datei die Zielhostumgebung oder die benötigte Analyse-VM nicht verfügbar ist.
Maximum Licenses (Maximale Lizenzen)	Geben Sie die Anzahl der Benutzerlizenzen an, über die Sie verfügen. Sie müssen auch das Betriebssystem und die Anwendungen in der Image-Datei berücksichtigen. Beachten Sie, dass die Image-Datei für einen Windows 7-Computer ist, auf dem Microsoft Office installiert ist. Angenommen, Sie verfügen über drei gleichzeitige Lizenzen für Windows 7 und zwei für Microsoft Office. In diesem Fall müssen Sie 2 als Anzahl der maximalen Lizenzen eingeben. Dies ist einer der Faktoren, die die Anzahl der gleichzeitigen Analyse-VMs bestimmen, die McAfee Advanced Threat Defense von der Image-Datei erstellt. Auf einer ATD-3000 werden maximal 30 Analyse-VMs und auf einer ATD-6000 maximal 60 Analyse-VMs unterstützt. Das bedeutet, dass der kumulative Wert der **Maximum Licenses** für alle VM-Profile einschließlich der Standard-Android-Analyse-VM im Falle einer ATD-3000 30 und im Falle einer ATD-6000 60 nicht übersteigen darf. Sie können also bei einer ATD-3000 über bis zu 29 und bei einer ATD-6000 über bis zu 59 Windows-Analyse-VMs verfügen. Die maximale Anzahl von Analyse-VMs, die Sie in eine McAfee Advanced Threat Defense Appliance hochladen können, hängt vom Windows-Betriebssystem und dem Appliance-Typen ab. • Windows Server 2008, Windows Server 2003 SP1/SP2, Windows 7 SP1 (64 Bit) und Windows 7 SP1 (32 Bit): bis zu 20 Analyse-VMs für ATD-3000 und bis zu 40 für ATD-6000. • Windows XP SP2/SP3: bis zu 30 Analyse-VMs für ATD-3000 und bis zu 60 für ATD-6000.
Speichern	Mit dem Befehl wird der VM-Profildatensatz mit den angegebenen Informationen erstellt. Wenn Sie auf **Speichern** klicken, startet die VM-Erstellung im Hintergrund als Daemon, und das VM-Profil wird auf der Seite "VM-Profil" aufgeführt. Auch wenn das neu erstellte VM-Profil auf der Seite **VM-Profil** aufgeführt ist, dauert es ca. 10 bis 15 Minuten, bis die Analyse-VM und das VM-Profil verwendet werden können.
Abbrechen	Der Befehl schließt die Seite **VM-Profil**, ohne die Änderungen zu speichern.

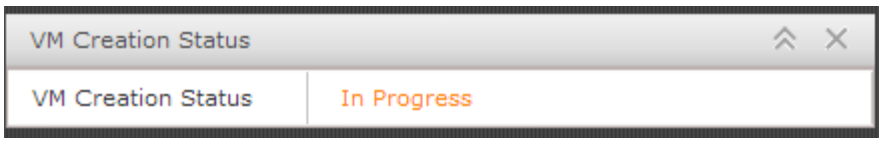
7 Überwachen Sie den Fortschritt der VM-Erstellung.

Es wird eine Meldung zur VM-Erstellung angezeigt.


Information
The VMs are being created and the VM Creation Status progress can be monitored in the Dashboard. Each VM will take about 5~10 minutes to complete
OK

Sie können den Fortschritt mithilfe der folgenden Methoden überwachen:

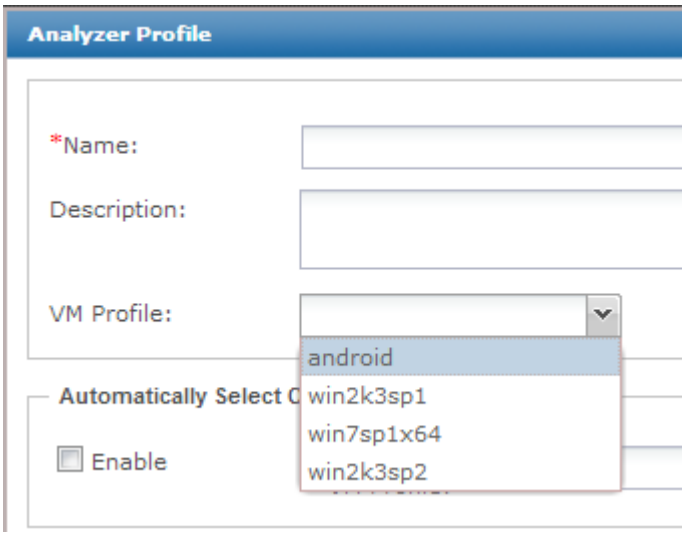
- Wählen Sie **Dashboard** aus, und überprüfen Sie den Monitor **VM Creation Status** (VM-Erstellungsstatus).



- Wählen Sie **Richtlinie** | **VM-Profil** aus, um den Status mit dem entsprechenden VM-Profil zu vergleichen.

Um die Systemprotokolle im Zusammenhang mit der VM-Erstellung anzuzeigen, wählen Sie **Verwalten** | **Systemprotokoll** aus.

8 Um die erfolgreiche Erstellung des VM-Profils zu bestätigen, wählen Sie **Richtlinie** | **Analyseprofil** aus, und überprüfen Se, ob das erstellte VM-Profil im Dropdown-Menü **VM-Profil** aufgeführt ist.



Bearbeiten von VM-Profilen

Bevor Sie beginnen
Zum Bearbeiten eines VM-Profils müssen Sie dieses entweder erstellt haben oder eine Administratorbenutzerrolle haben.

Vorgehensweise

1 Wählen Sie **Richtlinie** | **VM-Profil**.

Die verfügbaren VM-Profile werden aufgeführt.

2 Wählen Sie den gewünschten Datensatz aus, und klicken Sie auf **Bearbeiten**.

Die Seite **VM-Profil** wird angezeigt.

3 Nehmen Sie die Änderungen an den gewünschten Feldern vor, und klicken Sie auf **Speichern**.

Löschen von VM-Profilen

Bevor Sie beginnen

- Zum Löschen eines VM-Profils müssen Sie dieses entweder erstellt haben oder eine Administratorbenutzerrolle haben.
- Stellen Sie sicher, dass das zu löschende VM-Profil nicht in den Analyseprofilen festgelegt ist.

Vorgehensweise

1 Wählen Sie **Richtlinie** | **VM-Profil**.

Die verfügbaren VM-Profile werden angezeigt.

2 Wählen Sie den gewünschten Datensatz aus, und klicken Sie auf **Löschen**.

3 Klicken Sie auf **Ja**, um das Löschen zu bestätigen.

Anzeigen des VM-Erstellungsprotokolls

Wenn Sie auf der Seite **VM Profile** ein VM-Profil konfigurieren, erstellt McAfee Advanced Threat Defense eine Analyse-VM aus der Image-Datei, die Sie im VM-Profildatensatz ausgewählt haben. Gleichzeitig werden die dazugehörigen Protokolle ausgegeben, die Sie in der McAfee Advanced Threat Defense-Web-Anwendung anzeigen können. Mithilfe dieser Protokolleinträge sehen Sie die Vorgänge bei der Erstellung der Analyse-VM. Diese Informationen sind bei der Fehlerbehebung hilfreich.

Vorgehensweise

- Nachdem Sie auf der Seite **VM Profile** auf **Save** (Speichern) geklickt haben, wählen Sie **Verwalten** | **VM-Erstellungsprotokoll** , um die Protokolleinträge anzuzeigen.

  Die Protokolleinträge können nicht gedruckt oder exportiert werden.

6

Konfigurieren von McAfee Advanced Threat Defense für die Malware-Analyse

Nach der Installation der McAfee Advanced Threat Defense Appliance in Ihrem Netzwerk können Sie sie für die Malware-Analyse konfigurieren. Verwenden Sie dazu die McAfee Advanced Threat Defense-Web-Anwendung. Zum Konfigurieren der Malware-Analyse müssen Sie mindestens über die Webzugriffsrolle verfügen.

Dieser Abschnitt enthält die Terminologie und Vorgehensweisen zum Einrichten vonMcAfee Advanced Threat Defense für die Malware-Analyse.

Inhalt

- *Begriffe*
- *Grundlegende Schritte zum Konfigurieren der Malware-Analyse*
- *Wie analysiert McAfee Advanced Threat Defense Malware?*
- *Verwalten von Analyseprofilen*
- *Integration in McAfee ePO*
- *Integration in Data Exchange Layer*
- *Integration in McAfee Next Generation Firewall*
- *Konfigurieren des Proxy-Servers für die Internetverbindung*
- *Konfigurieren der Syslog-Einstellung*
- *Konfigurieren von DNS-Einstellungen*
- *Konfigurieren der Datums- und Uhrzeiteinstellungen*
- *Definieren von benutzerdefinierten YARA-Regeln zur Malware-Identifizierung*

Begriffe

Die Malware-Analyse mit McAfee Advanced Threat Defense wird erleichtert, wenn man die folgenden Begriffe kennt.

- **Static analysis** (Statische Analyse) – Wenn McAfee Advanced Threat Defense eine unterstützte Datei zur Analyse erhält, wird zuerst eine statische Analyse der Datei ausgeführt. Dabei wird in der kürzestmöglichen Zeit überprüft, ob es sich um bekannte Malware handelt, wobei die McAfee

Advanced Threat Defense-Ressourcen für die dynamische Analyse beibehalten werden. Für die statische Analyse verwendet McAfee Advanced Threat Defense die folgenden Ressourcen.

> Die statische Analyse wird in der nachstehenden Reihenfolge durchgeführt.
>
> 1. Lokale Whitelist > 2. Lokale Blacklist >3. McAfee GTI / McAfee Gateway Anti-Malware Engine / McAfee Anti-Malware Engine (Diese drei Ressourcen werden hintereinander bearbeitet.)

- **Local Whitelist** (Lokale Whitelist) – Dies ist die Liste der MD5-Hashwerte vertrauenswürdiger Dateien, die keiner Analyse bedürfen. Diese Whitelist basiert auf der McAfee® Application Control-Datenbank, die für andere Lösungen in der McAfee-Suite verwendet wird. Sie enthält über 230.000.000 Einträge.

  Die Whitelist-Funktion ist standardmäßig aktiviert. Verwenden Sie zum Deaktivieren den Befehl `setwhitelist`. Für die Verwaltung der Whitelist-Einträge stehen Befehle zur Verfügung. Die statische McAfee® Application Control-Datenbank kann nicht geändert werden. Sie können jedoch Einträge basierend auf dem Datei-Hash hinzufügen oder löschen. Sie können auch die Whitelist nach einem bestimmten Datei-Hash abfragen, um festzustellen, ob er der Datenbank hinzugefügt wurde.

  > Die Standardeinträge der Whitelist werden nicht regelmäßig aktualisiert. Sie können jedoch beim Upgrade der McAfee Advanced Threat Defense-Software aktualisiert werden.

  Die McAfee-Produkte, die Dateien an McAfee Advanced Threat Defense senden, sind ebenfalls in der Lage, Dateien in die Whitelist aufzunehmen. Zu diesen Produkten zählen McAfee Web Gateway und McAfee Network Security Platform.

  Die Befehle finden Sie unter whitelist auf Seite 373.

- **Local Blacklist** (Lokale Blacklist) – Dies ist die Liste der MD5-Hashwerte bekannter Malware, die in der McAfee Advanced Threat Defense-Datenbank gespeichert sind. Wenn McAfee Advanced Threat Defense Malware über die heuristische McAfee Gateway Anti-Malware Engine oder die dynamische Analyse erkennt, wird die lokale Blacklist mit dem MD5-Hashwert aktualisiert. Eine Datei wird dieser Liste nur automatisch hinzugefügt, wenn von McAfee Advanced Threat Defense ein Malware-Schweregrad von mittel, hoch oder sehr hoch ermittelt wird. Für die Verwaltung der Blacklist-Einträge stehen Befehle zur Verfügung.

  Die Befehle finden Sie unter Blacklist auf Seite 349.

- **McAfee GTI** – Dies ist ein globales Korrelationsmodul für Bedrohungen und die zentrale Wissensdatenbank für globales Messaging- und Kommunikationsverhalten, die den Schutz vor bekannten und aufkommenden elektronischen Bedrohungen in allen Bereichen ermöglichen. Das Kommunikationsverhalten umfasst Reputation, Volumen und Netzwerkdatenverkehrsmuster. McAfee Advanced Threat Defense verwendet die IP-Reputations- und Datei-Reputationsfunktionen von GTI.

  > Damit Datei-Reputations-Abfragen erfolgreich sind, stellen Sie sicher, dass McAfee Advanced Threat Defense mit `tunnel.message.trustedsource.org` über HTTPS (TCP/443) kommunizieren kann. McAfee Advanced Threat Defense ruft die URL-Aktualisierungen von `List.smartfilter.com` über HTTP (TCP/80) ab.

- **Gateway Anti-Malware** – McAfeeGateway Anti-Malware Engine analysiert das Verhalten von Websites, Website-Code und heruntergeladenen Web 2.0-Inhalten in Echtzeit, um bösartige Angriffe präventiv zu erkennen und zu blockieren. Dadurch werden Unternehmen vor komplexen Angriffen wie Viren, Würmern, Adware, Spyware, Riskware und ähnlichen Crimeware-Bedrohungen geschützt, ohne auf Virussignaturen zurückgreifen zu müssen.

  McAfee Gateway Anti-Malware Engine ist in McAfee Advanced Threat Defense eingebettet, um Malware-Erkennung in Echtzeit zu liefern.

- **Anti-Malware** – McAfee Anti-Malware Engine ist in McAfee Advanced Threat Defense eingebettet. DAT-Aktualisierungen werden entweder manuell oder automatisch vorgenommen, basierend auf der Netzwerkverbindung von McAfee Advanced Threat Defense.

  Die statische Analyse schließt auch die Analyse des bösartigen Codes mittels Reverse Engineering ein. Dies umfasst die Analyse aller Anweisungen und Eigenschaften zur Erkennung des beabsichtigten Verhaltens, das möglicherweise nicht sofort ersichtlich ist. Dadurch werden detaillierte Informationen zur Malware-Klassifizierung bereitgestellt und der Schutz erweitert. Zudem kann zugehörige Malware identifiziert werden, die die Wiederverwendung von Code nutzt.



Standardmäßig lädt McAfee Advanced Threat Defense die Aktualisierungen für McAfee Gateway Anti-Malware Engine und McAfee Anti-Malware Engine alle 90 Minuten herunter. Verwenden Sie für eine sofortige Aktualisierung den CLI-Befehl update_avdat auf Seite 373. Damit diese Aktualisierungen erfolgreich sind, stellen Sie sicher, dass McAfee Advanced Threat Defense `wpm .webwasher.com` über HTTPS (TCP/443) kontaktieren kann.

- **Dynamic Analysis** (Dynamische Analyse) – Dabei führt McAfee Advanced Threat Defense die Datei auf einem sicheren virtuellen Computer (Virtual Machine, VM) aus und überwacht ihr Verhalten, um zu überprüfen, wie böswillig die Datei ist. Am Ende der Analyse wird je nach Bedarf ein detaillierter Bericht erstellt. McAfee Advanced Threat Defense führt nach Abschluss der statischen Analyse eine dynamische Analyse durch. Standardmäßig führt McAfee Advanced Threat Defense keine dynamische Analyse durch, wenn bei der statischen Analyse Malware erkannt wird. Sie können jedoch eine Durchführung der dynamischen Analyse unabhängig von den Ergebnissen der statischen Analyse in McAfee Advanced Threat Defense konfigurieren. Auch die Konfigurierung einer dynamischen Analyse ohne statische Analyse ist möglich. Die dynamische Analyse beinhaltet auch die Disassembly-Listenfunktion von McAfee Advanced Threat Defense. Diese Funktion kann den Disassembly-Code für PE-Dateien generieren, damit Sie die Probe weiter analysieren können.

- **Analyzer VM** (Analyse-VM) – Dies ist der virtuelle Computer auf der McAfee Advanced Threat Defense, der für dynamische Analysen verwendet wird. Zur Erstellung der Analyse-VMs müssen Sie die VMDK-Datei mit dem erforderlichen Betriebssystem und allen Anwendungen erstellen. Dann importieren Sie diese Datei über SFTP in die McAfee Advanced Threat Defense Appliance.

  Für das Erstellen der Analyse-VMs werden nur die folgenden Betriebssysteme unterstützt:

  - Microsoft Windows XP (32 Bit), Service Pack 2
  - Microsoft Windows XP (32 Bit), Service Pack 3
  - Microsoft Windows Server 2003 (32 Bit), Service Pack 1
  - Microsoft Windows Server 2003 (32 Bit), Service Pack 2
  - Microsoft Windows Server 2008 R2, Service Pack 1
  - Microsoft Windows 7 (32 Bit), Service Pack 1
  - Microsoft Windows 7 (64 Bit), Service Pack 1
  - Microsoft Windows 8.0 Pro (32 Bit)

- Microsoft Windows 8.0 Pro (64 Bit)
- Standardmäßig Android 2.3. Sie können ein Upgrade auf Android 4.3 durchführen. Siehe Upgrade der Android-Analyse-VM auf Seite 55.

Die oben genannten Windows-Betriebssysteme können auf Deutsch, Englisch, Chinesisch (vereinfacht), Japanisch oder Italienisch vorliegen.



Die einzige vorinstallierte Analyse-VM ist die Android-VM.

Für Windows müssen Sie selbst Analyse-VMs erstellen. Sie können verschiedene VMs abhängig von den jeweiligen Anforderungen erstellen. Die Anzahl der Analyse-VMs, die Sie erstellen können, wird nur vom Festplattenspeicher auf der McAfee Advanced Threat Defense Appliance begrenzt. Es gibt jedoch eine Beschränkung, wie viele VMs gleichzeitig für die Analyse verwendet werden können. Auch die Anzahl der gleichzeitig nutzbaren Lizenzen, die Sie festlegen, hat Auswirkungen auf die Anzahl der gleichzeitigen Instanzen für eine Analyse-VM.

- **VM Profile** (VM-Profil) – Nachdem Sie die VM-Laufwerksdatei (VMDK-Datei) auf McAfee Advanced Threat Defense hochgeladen haben, können Sie jede davon mit einem separaten VM-Profil verknüpfen. Ein VM-Profil gibt den installierten Inhalt einer VM-Laufwerksdatei und die Anzahl der gleichzeitigen Lizenzen, die mit der Datei verknüpft sind, an. Mithilfe der VM-Laufwerksdatei und der Informationen im VM-Profil erstellt McAfee Advanced Threat Defense die entsprechende Anzahl an Analyse-VMs. Wenn Sie beispielsweise angeben, dass Sie über 10 Lizenzen für Windows XP SP2 (32 Bit) verfügen, versteht McAfee Advanced Threat Defense, dass bis zu 10 gleichzeitige VMs mit der VMDK-Datei erstellt werden können.
- **Analyzer profile** (Analyseprofil) – Dieses legt fest, wie eine Datei analysiert wird und welche Informationen im Bericht stehen. In einem Analyse-Profil konfigurieren Sie Folgendes:
  - VM-Profil
  - Analyseoptionen
  - Berichte, die nach der Analyse angezeigt werden sollen
  - Kennwort für Probedateien im ZIP-Format
  - Mindest- und Höchstausführungszeit für die dynamische Analyse

  Sie können mehrere Analyseprofile abhängig von den jeweiligen Anforderungen erstellen. Für jeden McAfee Advanced Threat Defense-Benutzer müssen Sie ein Standardanalyseprofil festlegen. Dieses Analyseprofil wird für alle Dateien verwendet, die vom Benutzer hochgeladen werden. Benutzer, die die McAfee Advanced Threat Defense-Web-Anwendung zum manuellen Hochladen von Dateien für die Analyse verwenden, können für den Datei-Upload ein anderes Analyseprofil wählen. Das für eine Datei ausgewählte Analyseprofil hat Vorrang vor dem Standardanalyseprofil des jeweiligen Benutzers.

Um eine Datei dynamisch zu analysieren, muss der Benutzer das VM-Profil haben, das in seinem Analyseprofil angegeben ist. Auf diese Weise legt der Benutzer die Umgebung fest, in der McAfee Advanced Threat Defense die Datei ausführen soll. Sie können auch ein Standard-VM-Profil für 32-Bit- und 64-Bit-Windows erstellen.

- **User** (Benutzer) – Ein McAfee Advanced Threat Defense-Benutzer verfügt über die erforderlichen Berechtigungen, um Dateien zur Analyse und Anzeige der Ergebnisse an McAfee Advanced Threat Defense zu senden. Im Fall der manuellen Übertragung kann ein Benutzer die McAfee Advanced Threat Defense-Web-Anwendung oder einen FTP-Client verwenden. Im Fall der automatischen Übertragung integrieren Sie McAfee Advanced Threat Defense in McAfee-Produkte wie McAfee Network Security Platform oder McAfee Web Gateway. Wenn diese Produkte einen Datei-Download erkennen, senden Sie die Datei automatisch an McAfee Advanced Threat Defense, bevor der Download abgeschlossen werden kann. Für diese Produkte sind Standardbenutzerprofile in McAfee Advanced Threat Defense verfügbar.

  Für jeden Benutzer definieren Sie das Standardanalyseprofil, das wiederum das VM-Profil enthalten kann. Wenn Sie McAfee Advanced Threat Defense zum Hochladen von Dateien für die Analyse verwenden, können Sie dieses Standardprofil für die Dateiübertragung außer Kraft setzen. Für andere Benutzer verwendet McAfee Advanced Threat Defense die Standardprofile.

Grundlegende Schritte zum Konfigurieren der Malware-Analyse

In diesem Abschnitt erfahren Sie Näheres über die wichtigsten Schritte zum Konfigurieren von McAfee Advanced Threat Defense für die Malware-Analyse und Malware-Berichte:

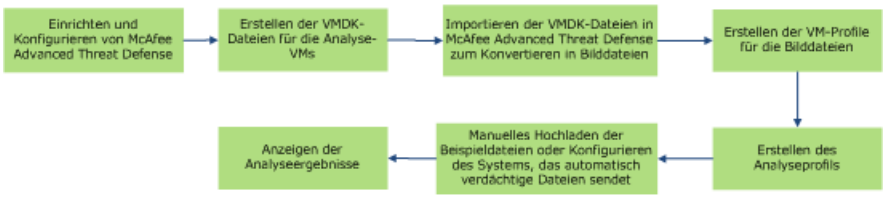

Einrichten und Konfigurieren von McAfee Advanced Threat Defense
Erstellen der VMDK-Dateien für die Analyse-VMs
Importieren der VMDK-Dateien in McAfee Advanced Threat Defense zum Konvertieren in Bilddateien
Erstellen der VM-Profile für die Bilddateien
Erstellen des Analyseprofils
Manuelles Hochladen der Beispieldateien oder Konfigurieren des Systems, das automatisch verdächtige Dateien sendet
Anzeigen der Analyseergebnisse

Abbildung 6-1 Zusammenfassung der Schritte zum Konfigurieren der Malware-Analyse

1 Richten Sie die McAfee Advanced Threat Defense Appliance ein, und vergewissern Sie sich, dass Sie ordnungsgemäß läuft.

   - Stellen Sie sicher, dass die McAfee Advanced Threat Defense Appliance über die erforderlichen Netzwerkverbindungen für Ihre Bereitstellungsoption verfügt. Beispiel: Wenn Sie eine Integration in Network Security Platform durchführen, vergewissern Sie sich, dass Sensor, Manager und McAfee Advanced Threat Defense Appliance miteinander kommunizieren können.
   - Vergewissern Sie sich, dass die erforderlichen Module für die statische Analyse, beispielsweise McAfee Gateway Anti-Malware Engine, auf dem aktuellen Stand sind.

2 Erstellen Sie die Analyse-VMs und die VM-Profile. Siehe Erstellen einer Analyse-VM auf Seite 4.

3 Erstellen Sie die benötigten Analyseprofile. Siehe Verwalten von Analyseprofilen auf Seite 251.

4 Falls Sie möchten, dass McAfee Advanced Threat Defense die Ergebnisse auf einen FTP-Server hochlädt, konfigurieren Sie diese Option, und halten Sie die Details dazu bereit, bevor Sie die Profile für die entsprechenden Benutzer erstellen.

5 Erstellen Sie die erforderlichen Benutzerprofile. Siehe Hinzufügen von Benutzern auf Seite 40.

6 Melden Sie sich mithilfe der Anmeldeinformationen eines von Ihnen erstellten Benutzers bei der McAfee Advanced Threat Defense-Web-Anwendung an, und laden Sie eine Probedatei zur Analyse hoch. Dieser Schritt dient der Überprüfung, dass McAfee Advanced Threat Defense ordnungsgemäß konfiguriert ist. Siehe Hochladen von Dateien zur Analyse mittels McAfee Advanced Threat Defense-Web-Anwendung auf Seite 280.

7 Überwachen Sie auf der Seite **Analysestatus** den Status der Analyse. Siehe Konfigurieren der Seite "Analysis Status" (Analysestatus) auf Seite 290.

8 Zeigen Sie nach Abschluss der Analyse den Bericht auf der Seite **Analysis Results** (Analyseergebnisse) an. Siehe Anzeigen der Analyseergebnisse auf Seite 294.

Wie analysiert McAfee Advanced Threat Defense Malware?

In diesem Abschnitt lernen Sie den typischen Workflow von McAfee Advanced Threat Defense beim Analysieren von Dateien auf Malware kennen.

Stellen Sie sich folgende Situation vor: Sie haben eine Datei manuell mithilfe der McAfee Advanced Threat Defense-Web-Anwendung hochgeladen.

1 Wir gehen davon aus, dass das Dateiformat unterstützt wird. McAfee Advanced Threat Defense entpackt die Datei und berechnet den MD5-Hashwert.

2 McAfee Advanced Threat Defense wendet das während des Hochladens angegebene Analyseprofil an.

3 Auf Basis der Konfiguration im Analyseprofil bestimmt die Lösung die Module für die statische Analyse und gleicht die Datei gegen diese Module ab.

4 Ergibt die statische Analyse, dass die Datei bösartig ist, führt McAfee Advanced Threat Defense keine weiteren Analysen aus und generiert die erforderlichen Berichte. Dies ist jedoch abhängig davon, wie Sie das entsprechende Analyseprofil konfiguriert haben.

5 Falls die statische Analyse keine Malware erkennt oder Sie McAfee Advanced Threat Defense zur Ausführung einer dynamischen Analyse unabhängig von den statischen Analyseergebnissen konfiguriert haben, startet McAfee Advanced Threat Defense die dynamische Analyse der Datei.

6 Die Lösung führt die Datei auf der entsprechenden Analyse-VM aus und erstellt Aufzeichnungen über alle Verhaltensweisen. Die Analyse-VM wird durch das VM-Profil im Analyseprofil bestimmt.

7 Wenn die Datei vollständig ausgeführt oder die maximale Ausführungszeit erreicht wurde, erstellt McAfee Advanced Threat Defense die erforderlichen Berichte.

8 Nach dem Abschluss der dynamischen Analyse setzt die Lösung die Analyse-VM auf die Basisversion zurück, sodass sie zur Analyse der nächsten Datei in der Warteschlange zur Verfügung steht.

Internetzugriff für Probedateien

Während einer dynamischen Analyse einer Probe könnte diese auf eine Ressource im Internet zugreifen. Zum Beispiel könnte die Probe versuchen, zusätzlichen bösartigen Code herunterladen oder auf dem Host-Computer (in diesem Fall auf der Analyse-VM) gesammelte Informationen hochzuladen. Sie können McAfee Advanced Threat Defense so konfigurieren, dass den Analyse-VMs Netzwerkdienste bereitgestellt werden, damit die Netzwerkaktivitäten einer Probedatei analysiert werden können.

Erhalten Proben Zugriff auf das Internet, kann McAfee Advanced Threat Defense das Netzwerkverhalten einer Probe analysieren und die Auswirkungen der zusätzlich aus dem Internet heruntergeladenen Dateien ermitteln. Einige Malware-Programme könnten versuchen, festzustellen, ob sie in einer Sandkastenumgebung ausgeführt werden, indem sie einen Zugriff auf das Internet vornehmen und gegebenenfalls ihr Verhalten ändern.

Wenn eine Analyse-VM erstellt wird, sorgt McAfee Advanced Threat Defense dafür, dass die Analyse-VM über die für eine Kommunikation über ein Netzwerk erforderlichen Konfigurationen verfügt.

Mithilfe einer Einstellung in den Analyseprofilen können Sie einer Analyse-VM den Netzwerkzugriff erlauben. Netzwerkdienste werden unabhängig von der für das Senden der Probe verwendeten Methode bereitgestellt. Zum Beispiel erhalten sowohl manuell über die McAfee Advanced Threat Defense-Web-Anwendung gesendete Proben als auch jene, die von integrierten Produkten gesendet wurden, Netzwerkzugriff.

Im Folgenden finden Sie den grundlegenden Prozessablauf für den Zugriff einer Probe auf eine Ressource im Internet.

1. Eine Probe versucht, auf eine Ressource im Internet zuzugreifen.
2. McAfee Advanced Threat Defense überprüft, ob im für die Analyse verwendeten Profil die Option für eine Internetverbindung aktiviert ist.
3. Je nachdem, ob die Option für eine Internetverbindung aktiviert ist oder nicht, bestimmt McAfee Advanced Threat Defense den Modus für die Bereitstellung von Netzwerkdiensten.
   - Simulationsmodus – Wenn die Option für eine Internetverbindung nicht im Analyseprofil aktiviert ist, wird dieser Modus verwendet. McAfee Advanced Threat Defense kann selbst als Zielressource fungieren. Versucht die Probe zum Beispiel, eine Datei über FTP herunterzuladen, simuliert McAfee Advanced Threat Defense die Verbindung für die Analyse-VM.
   - Real Internet-Modus – Bei diesem Modus ist für den Verwaltungsport (ETH-0), ETH-1, ETH-2 oder ETH-3 Internetzugriff erforderlich. Wenn die Option für eine Internetverbindung im Analyseprofil aktiviert ist, verwendet McAfee Advanced Threat Defense diesen Modus. McAfee Advanced Threat Defense stellt eine echte Internetverbindung standardmäßig über den Verwaltungsport her, der öffentlich oder gemäß Ihrer Netzwerkkonfiguration zur Firewall Ihres Unternehmens geleitet wird. Da der Datenverkehr von einer Analyse-VM bösartig sein kann, sollten Sie diesen Datenverkehr eventuell von Ihrem Produktionsnetzwerk trennen. In diesem Fall können Sie ETH-1, ETH-2 oder ETH-3 von McAfee Advanced Threat Defense verwenden oder der Analyse-VM den Internetzugriff erlauben.

4 Unabhängig vom verwendeten Modus protokolliert McAfee Advanced Threat Defense alle Netzwerkaktivitäten. Die generierten Berichttypen können jedoch je nach Modus unterschiedlich ausfallen.

- Im Übersichtsbericht der Analyse werden die Netzwerkaktivitäten zusammengefasst und dargestellt. Unter den Netzwerkvorgängen finden Sie die DNS-Abfragen und Socketaktivitäten. Alle Netzwerkaktivitäten finden Sie im Abschnitt **Network Simulator** (Netzwerksimulator) des Berichts.
- Der Bericht "dns.log" enthält ebenfalls die DNS-Abfragen der Probe.
- Die Paketerfassung der Netzwerkaktivitäten finden Sie im Ordner "NetLog" der ZIP-Datei "Complete Results" (Vollständige Ergebnisse).

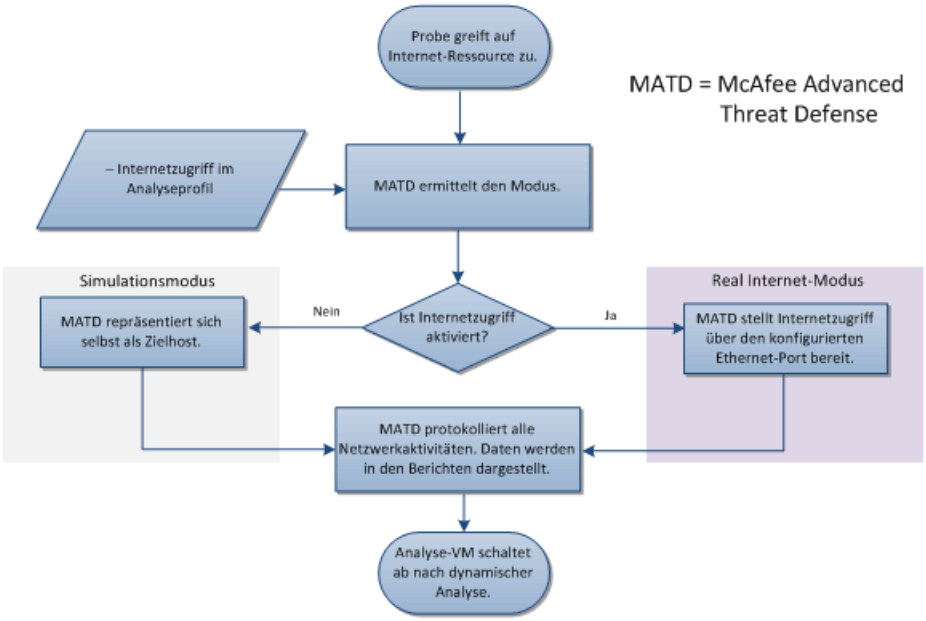

Probe greift auf Internet-Ressource zu.
MATD = McAfee Advanced Threat Defense
– Internetzugriff im Analyseprofil
MATD ermittelt den Modus.
Simulationsmodus
Real Internet-Modus
Nein
Ist Internetzugriff aktiviert?
Ja
MATD repräsentiert sich selbst als Zielhost.
MATD stellt Internetzugriff über den konfigurierten Ethernet-Port bereit.
MATD protokolliert alle Netzwerkaktivitäten. Daten werden in den Berichten dargestellt.
Analyse-VM schaltet ab nach dynamischer Analyse.

Abbildung 6-2 Internetzugriff für Proben – Prozessablauf

Beachten Sie Folgendes: McAfee Advanced Threat Defense verwendet standardmäßig den Verwaltungsport (ETH-0), um Proben den Zugriff auf das Internet zu erlauben. Sie können für diesen Zweck auch einen anderen Port konfigurieren.

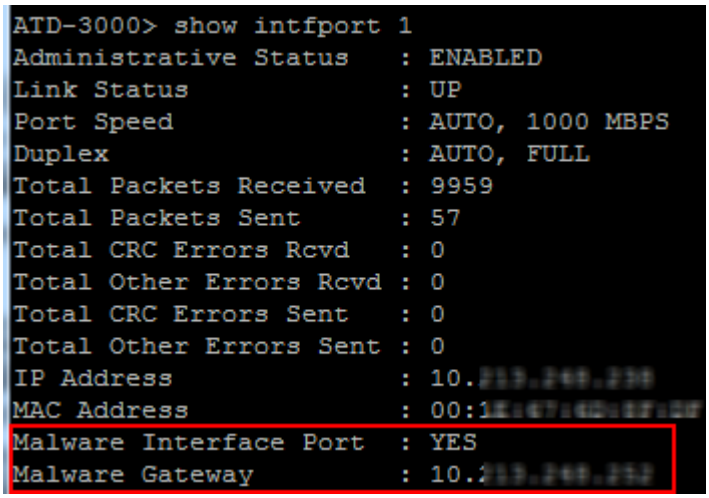
Um einen anderen Ethernet-Port für den Malware-Netzwerkzugriff zu aktivieren, führen Sie die unten beschriebenen Schritte aus:

1 Melden Sie sich bei der McAfee Advanced Threat Defense-CLI an, und aktivieren Sie den gewünschten Port. Zum Beispiel aktivieren Sie den ETH-1-Port mit `set intfport 1 enable`.

2 Legen Sie die gewünschte IP-Adresse und Subnetzmaske für den Port fest. Beispiel: `set intfport 1 10.10.10.10 255.255.255.0`

3 Legen Sie für den Ethernet-Port das Gateway fest, worüber der Internetzugriff geleitet werden soll. Beispiel: `set malware-intfport 1 gateway 10.10.10.252`

4 Führen Sie den Befehl `show intfport <port number>` für den Port aus, um zu überprüfen, ob er für den Malware-Internetzugriff konfiguriert ist. Beispiel: `show intfport 1`. Überprüfen Sie die Einträge für `Malware Interface Port` und `Malware Gateway`.


ATD-3000> show intfport 1
Administrative Status : ENABLED
Link Status : UP
Port Speed : AUTO, 1000 MBPS
Duplex : AUTO, FULL
Total Packets Received : 9959
Total Packets Sent : 57
Total CRC Errors Rcvd : 0
Total Other Errors Rcvd : 0
Total CRC Errors Sent : 0
Total Other Errors Sent : 0
IP Address : 10.
MAC Address : 00:
Malware Interface Port : YES
Malware Gateway : 10.

- Um für den Malware-Internetzugriff wieder den Verwaltungsport (ETH-0) zu verwenden, führen Sie in der CLI den Befehl `set malware-intfport mgmt` aus. McAfee Advanced Threat Defense verwendet die Verwaltungsport-IP und das entsprechende Standard-Gateway, um Proben den Zugriff auf das Internet zu erlauben.
- Nehmen wir an, dass Sie für den Malware-Internetzugriff ETH-1 konfiguriert haben, aber nun ETH-2 verwenden möchten. Führen Sie dann die oben genannten Schritte für ETH-2 aus. ETH-2 wird als Port für den Malware-Internetzugriff festgelegt.
- Nehmen wir an, dass Sie für den Malware-Internetzugriff ETH-1 konfiguriert haben, aber nun ETH-1 mit einer anderen IP-Adresse oder einem anderen Gateway verwenden möchten. Führen Sie dann die Schritte mit der neuen IP-Adresse bzw. dem neuen Gateway aus.
- Der Befehl `route add network` gilt für den allgemeinen Datenverkehr von Advanced Threat Defense. `set malware-intfport` gilt hingegen für den Internet-Datenverkehr einer Analyse-VM. Daher wirken sich die Befehle `route add network` und `set malware-intfport` nicht aufeinander aus.

Verwalten von Analyseprofilen

Wenn eine Datei manuell oder automatisch zur Analyse an McAfee Advanced Threat Defense gesendet wird, wird das entsprechende Analyseprofil verwendet, um festzustellen, wie die Datei analysiert werden muss und welche Ergebnisse im Analysebericht aufgeführt werden. Das VM-Profil wird im Analyseprofil festgelegt. Außerdem legen Sie fest, wie die Datei auf Malware analysiert und die Berichte veröffentlicht werden sollen. Somit enthält ein Analyseprofil alle wichtigen Benutzerkonfigurationen zur Analyse einer Datei.

Zur Verwaltung von Analyseprofilen verwenden Sie die McAfee Advanced Threat Defense-Web-Anwendung.

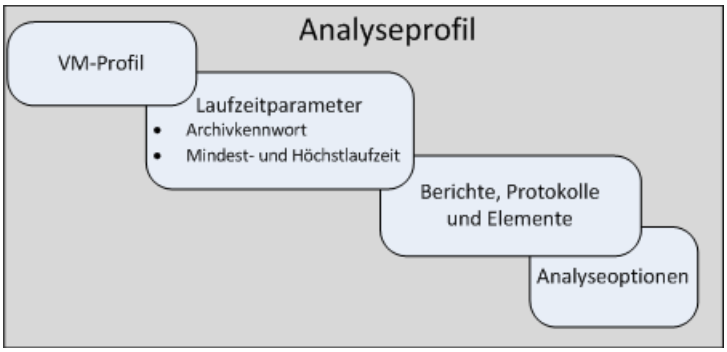


Abbildung 6-3 Inhalt eines Analyseprofils

Anzeigen der Analyseprofile

Abhängig von Ihrer Benutzerrolle können Sie die vorhandenen Analyseprofile in der McAfee Advanced Threat Defense-Web-Anwendung anzeigen.

Vorgehensweise

1 Wählen Sie **Richtlinie** | **Analyseprofil**.

Beim Web-Zugriff können Sie nur die von Ihnen erstellten Analyseprofile anzeigen. Wenn Sie über Administratorzugriff verfügen, können Sie alle Analyseprofile in der Datenbank anzeigen.

Spaltenname	Beschreibung
Auswählen	Dient zum Bearbeiten oder Löschen des entsprechenden Analyseprofils.
Name	Der von Ihnen zugewiesene Name des Analyseprofils.
Beschreibung	Die Beschreibung der Merkmale im Analyseprofil.
OS Name (Betriebssystemname)	Entspricht dem Namen des VM-Profils, das im Analyseprofil festgelegt wurde.
Automatically Select OS (Betriebssystem automatisch wählen)	Zeigt an, ob Sie die Option **Automatically Select OS** im Analyseprofil ausgewählt haben.

2 Blenden Sie die überflüssigen Spalten aus.

a Bewegen Sie den Mauszeiger über die rechte Ecke einer Spaltenüberschrift, und klicken Sie auf den Dropdown-Pfeil.

b Wählen Sie **Columns** (Spalten).

c Wählen Sie nur die erforderlichen Spaltennamen aus der Liste.

Sie können auf eine Spaltenüberschrift klicken und sie an die gewünschte Position ziehen.

3 Zum Sortieren der Datensätze basierend auf einem bestimmten Spaltennamen klicken Sie auf die Spaltenüberschrift.

Sie können die Datensätze in auf- oder absteigender Reihenfolge sortieren. Alternativ können Sie den Mauszeiger über die rechte Ecke einer Spaltenüberschrift bewegen und auf den Dropdown-Pfeil klicken. Wählen Sie dann **Sort Ascending** (Aufsteigend sortieren) oder **Sort Descending** (Absteigend sortieren).

4 Zum Anzeigen der vollständigen Details eines bestimmten Analyseprofils wählen Sie den Datensatz aus, und klicken Sie auf **View** (Anzeigen).

Erstellen von Analyseprofilen

Bevor Sie beginnen

- Wenn Sie die Option für die dynamische Analyse im Analyseprofil verwenden möchten, stellen Sie sicher, dass Sie das erforderliche VM-Profil erstellt haben. VM-Profile sind auch erforderlich, wenn Sie die Option **Automatically Select OS** (Betriebssystem automatisch wählen) verwenden möchten.
- Wenn Sie Proben Internetzugriff gewähren möchten, müssen Sie über Administratorbenutzerrechte verfügen.

Vorgehensweise

1 Wählen Sie **Richtlinie** | **Analyseprofil** | **Neu**.

Die Seite **Analyseprofil** wird angezeigt.

2 Geben Sie die entsprechenden Informationen in die jeweiligen Felder ein.

Optionsname	Beschreibung
Name	Geben Sie den Namen für das Analyseprofil ein. Wählen Sie einen Namen, der die Eigenschaften des Analyseprofils widerspiegelt.
Beschreibung	Optional können Sie auch eine detaillierte Beschreibung des Analyseprofils bereitstellen.
VM-Profil	Wählen Sie das VM-Profil, das McAfee Advanced Threat Defense für die dynamische Analyse einer Datei verwenden soll.
Automatically Select OS (Betriebssystem automatisch wählen)	Wenn McAfee Advanced Threat Defense automatisch das richtige VM-Profil für Windows 32 Bit und Windows 64 Bit wählen soll, klicken Sie auf **Enable** (Aktivieren), und wählen Sie anschließend die VM-Profile aus den Optionen **Windows 32-bit VM Profile** und **Windows 64-bit VM Profile** (VM-Profile für Windows 32 Bit und 64 Bit). Unter **VM Profile** haben Sie beispielsweise "Android" ausgewählt. Sie haben die Option **Automatically Select OS** (Betriebssystem automatisch wählen) aktiviert. Sie haben für **Windows 32-bit VM Profile** "Windows XP SP3" und für **Windows 64-bit VM Profile** "Windows 7 SP1 64 Bit" ausgewählt. Wird eine APK-Datei erkannt, wird nun automatisch die Android-Analyse-VM zur dynamischen Analyse der Datei verwendet. Ebenso wird für eine PE32-Datei Windows XP SP3 verwendet. Für eine PE64-Datei wird eine Analyse-VM mit Windows 7 SP1 64 Bit verwendet. Wenn McAfee Advanced Threat Defense das Betriebssystem für das Analyseprofil nicht bestimmen kann oder wenn die festgelegte Analyse-VM nicht verfügbar ist, wird die im Feld **VM Profile** (VM-Profil) angegebene VM verwendet.
Archive Password (Archivkennwort)	Geben Sie das Kennwort für McAfee Advanced Threat Defense ein, um eine kennwortgeschützte Malware-Probe zu entpacken.
Confirm Password (Kennwort bestätigen)	Geben Sie das Kennwort zur Bestätigung erneut ein.
Minimum Run Time (sec) (Mindestlaufzeit in Sekunden)	Geben Sie die Mindestdauer für die dynamische Analyse der Probe durch McAfee Advanced Threat Defense an. Der Standardwert ist 5 Sekunden. Der zulässige Höchstwert beträgt 600 Sekunden. Wenn das Ausführen der Datei vor diesem Zeitpunkt beendet ist, wird die dynamische Analyse angehalten.
Maximum Run Time (sec) (Maximale Laufzeit in Sekunden)	Geben Sie die maximale Dauer für die dynamische Analyse der Probe durch McAfee Advanced Threat Defense an. Der Standardwert beträgt 180 Sekunden. Der zulässige Höchstwert beträgt 600 Sekunden. Wenn das Ausführen der Datei vor diesem Zeitpunkt nicht beendet ist, wird die dynamische Analyse angehalten.
Analysis Summary (Analyseübersicht)	Wählen Sie diese Option, um den Übersichtsbericht der Analyse in die Analyseergebnisse aufzunehmen. Siehe Anzeigen des Berichts "Analysis Summary" (Analyseübersicht) auf Seite 297.
Packet captures (Paketaufzeichnungen)	Wählen Sie diese Option zum Aufzeichnen der Netzwerkpakete, falls die Datei während der dynamischen Analyse versucht, eine Kommunikation herzustellen. Die PCAP-Datei finden Sie in der "Complete Results" (Vollständige Ergebnisse).
Dropped Files (Betroffene Dateien)	Wählen Sie diese Option, um den Bericht "Files Created in Sandbox" (In Sandkastenumgebung erstellte Dateien) zu generieren. Siehe Bericht zu betroffenen Dateien auf Seite 304.

Optionsname	Beschreibung
Disassembly Results (Disassembly-Ergebnisse)	Wählen Sie diese Option, wenn McAfee Advanced Threat Defense den Disassembly-Code für PE-Dateien generieren soll. Siehe Disassembly-Ergebnisse auf Seite 304.
Logic Path Graph (Logisches Pfaddiagramm)	Wählen Sie diese Option, um den Bericht "Logic Path Graph" (Logisches Pfaddiagramm) zu generieren. Siehe Bericht "Logic Path Graph" (Logisches Pfaddiagramm) auf Seite 305.
User API Log (User API-Protokoll)	Dieser Bericht stellt Windows-DLL-API-Aufrufe auf Benutzerebene zur Verfügung, die während der dynamischen Analyse direkt von der Malware-Probe ausgeführt werden. Siehe User API-Protokoll auf Seite 310.
Local Black List (Lokale Blacklist)	Wählen Sie diese Option, wenn McAfee Advanced Threat Defense den MD5-Hashwert der Datei mit den MD5-Hashwerten auf der Blacklist der lokalen Datenbank abgleichen soll.
Anti-Malware (Malware-Schutz)	Wählen Sie diese Option, wenn McAfee Advanced Threat Defense die Datei mithilfe der McAfee Anti-Malware Engine überprüfen soll.
GTI File Reputation (GTI-Datei-Reputation)	Wählen Sie diese Option, wenn McAfee Advanced Threat Defense den MD5-Hashwert der Datei mit McAfee GTI abgleichen soll. Stellen Sie sicher, dass McAfee Advanced Threat Defense mit McAfee GTI (in der Cloud) kommunizieren kann.
Gateway Anti-Malware	Wählen Sie diese Option, wenn McAfee Advanced Threat Defense die Datei mithilfe der McAfee Gateway Anti-Malware Engine überprüfen soll.
Sandbox (Sandkasten)	Wählen Sie diese Option, wenn die Datei dynamisch analysiert werden soll. Eine Datei wird nicht dynamisch analysiert, wenn eine der statischen Methoden sie als Malware oder sichere Datei meldet. Wenn Sie die Datei unabhängig vom Ergebnis der statischen Analyse dynamisch analysieren möchten, wählen Sie auch **Run All Selected** (Gesamte Auswahl ausführen) aus. Stellen Sie sicher, dass Sie das VM-Profil und die **Runtime Parameters** (Laufzeitparameter) ausgewählt haben.
Run All Selected (Gesamte Auswahl ausführen)	Wählen Sie diese Option, wenn McAfee Advanced Threat Defense die Datei mithilfe aller ausgewählten Analyseoptionen analysieren soll, unabhängig vom Ergebnis einer bestimmten Methode.
Enable Malware Internet Access (Malware-Internetzugriff aktivieren)	Aktivieren Sie diese Option, um Proben Internetzugriff zu gewähren, wenn diese versuchen, auf eine Ressource im Internet zuzugreifen. Zum Aktivieren dieser Option muss die Option **Sandbox** (Sandkasten) unter "Analyzer Options" (Analyseoptionen) aktiviert sein. Sie müssen zudem über Administratorberechtigungen verfügen, um die Option **Enable Malware Internet Access** (Malware-Internetzugriff aktivieren) zu aktivieren bzw. zu deaktivieren. Da es sich bei der zu analysierenden Probe möglicherweise um Malware handelt, besteht beim Aktivieren der Option **Enable Malware Internet Access** (Malware-Internetzugriff aktivieren) die Gefahr, dass bösartiger Datenverkehr aus Ihrem Netzwerk heraus verbreitet wird. Beim Aktivieren dieser Option wird eine Haftungsausschlussmeldung angezeigt. Klicken Sie auf **OK**, um fortzufahren. Der Administrator kann zudem eine Proxy-Einstellung für Malware konfigurieren, sofern im Netzwerk ein Proxy-Server vorhanden ist.

Optionsname	Beschreibung
Speichern	Erstellt den Analyseprofil-Datensatz mit den von Ihnen bereitgestellten Informationen.
Abbrechen	Schließt die Seite **Analyseprofil**, ohne die Änderungen zu speichern.

Bearbeiten von Analyseprofilen

Vorgehensweise

1 Wählen Sie **Richtlinie** | **Analyseprofil**.

Beim Web-Zugriff können Sie nur die von Ihnen erstellten Analyseprofile anzeigen. Wenn Sie über Administratorzugriff verfügen, können Sie alle Analyseprofile in der Datenbank anzeigen.

2 Wählen Sie den gewünschten Datensatz aus, und klicken Sie auf **Bearbeiten**.

Die Seite **Analyseprofil** wird angezeigt.

3 Nehmen Sie die Änderungen an den gewünschten Feldern vor, und klicken Sie auf **Speichern**.

Die Änderungen haben Auswirkungen auf die entsprechenden Benutzer, selbst wenn sie derzeit nicht angemeldet sind.

Löschen von Analyseprofilen

Bevor Sie beginnen

Stellen Sie sicher, dass Benutzer, denen Sie dieses Analyseprofil zugewiesen haben, derzeit nicht bei McAfee Advanced Threat Defense angemeldet sind.

Vorgehensweise

1 Wählen Sie **Richtlinie** | **Analyseprofil**.

Beim Web-Zugriff können Sie nur die von Ihnen erstellten Analyseprofile anzeigen. Wenn Sie über Administratorzugriff verfügen, können Sie alle Analyseprofile in der Datenbank anzeigen.

2 Wählen Sie den gewünschten Datensatz aus, und klicken Sie auf **Löschen**.

3 Klicken Sie auf **Ja**, um das Löschen zu bestätigen.

Integration in McAfee ePO

Durch die Integration von McAfee Advanced Threat Defense in McAfee ePO kann McAfee Advanced Threat Defense die Zielhostumgebung korrekt identifizieren und die passendste Analyse-VM für die dynamische Analyse auswählen.

Zum Bestimmen der Analyse-VM für eine durch Network Security Platform oder McAfee Web Gateway gesendete Datei verwendet McAfee Advanced Threat Defense die folgenden Informationsquellen in der angeführten Reihenfolge:

1. McAfee Advanced Threat Defense fragt von McAfee ePO das Betriebssystem eines Hosts auf Basis von dessen IP-Adresse ab. Falls bei dieser Quelle keine Informationen oder keine entsprechende Analyse-VM vorhanden sind, wird mit der nächsten Quelle fortgefahren.
2. Wenn die Geräteprofilerstellung aktiviert ist, stellt der Sensor das Betriebssystem und die Anwendungen beim Weiterleiten einer Analyse zur Datei bereit. Falls bei dieser Quelle keine Informationen oder keine entsprechende Analyse-VM vorhanden sind, wird mit der nächsten Quelle fortgefahren.
3. Die McAfee Advanced Threat Defense bestimmt das VM-Profil auf Basis des Analyseprofils im entsprechenden Benutzerdatensatz. Falls bei dieser Quelle keine Informationen oder keine entsprechende Analyse-VM vorhanden sind, wird mit der nächsten Quelle fortgefahren.
4. Das als Standard ausgewählte VM-Profil. Sie können aus den VM-Profilen in der Konfiguration eines als Standard auswählen.

Wenn McAfee Advanced Threat Defense von McAfee ePO Hostdaten für eine bestimmte IP-Adresse erhält, werden diese im Cache zwischengespeichert.

- Die für die Hostdaten zwischengespeicherte IP-Adresse hat einen TTL-Wert (Time to Live-Wert, Gültigkeitsdauer) von 48 Stunden.
- Während der ersten 24 Stunden verwendet McAfee Advanced Threat Defense nur die Hostdaten aus dem Cache.
- Während der zweiten 24 Stunden, also von 24 bis 48 Stunden, verwendet McAfee Advanced Threat Defense die Hostdaten aus dem Cache und fragt McAfee ePO ab, um den Cache zu aktualisieren. Diese aktualisierten Daten gelten für die nächsten 48 Stunden.
- Wenn die zwischengespeicherten Daten älter als 48 Stunden sind, reagiert das System so, als wären keine zwischengespeicherten Daten für die IP-Adresse vorhanden. Das bedeutet, dass es versucht, die Informationen von anderen Quellen abzufragen, und es sendet auch eine Abfrage an McAfee ePO.

Nachfolgend wird beschrieben, wie McAfee Advanced Threat Defense mit McAfee ePO zusammenarbeitet.

1. Network Security Platform oder McAfee Web Gateway sendet eine Datei zur Analyse an McAfee Advanced Threat Defense. Beim Senden einer Datei durch Network Security Platform wird auch die IP-Adresse des Zielhosts gesendet.
2. McAfee Advanced Threat Defense überprüft den eigenen Cache, um herauszufinden, ob der IP-Adresse ein gültiges Betriebssystem zugeordnet ist.
3. Wenn diese Datei zum ersten Mal für diese IP-Adresse analysiert wird, gibt es keine Daten im Cache. Die Analyse-VM wird deshalb im Fall von Network Security Platform über die Geräteprofilinformationen und im Fall von McAfee Web Gateway über den Benutzerdatensatz ermittelt. Gleichzeitig wird eine Abfrage nach den Hostdaten für die IP-Adresse an McAfee ePO gesendet.
4. McAfee ePO leitet die Hostdaten an McAfee Advanced Threat Defense weiter, wo sie zur zukünftigen Verwendung im Cache zwischengespeichert werden.

Konfigurieren der McAfee ePO-Integration

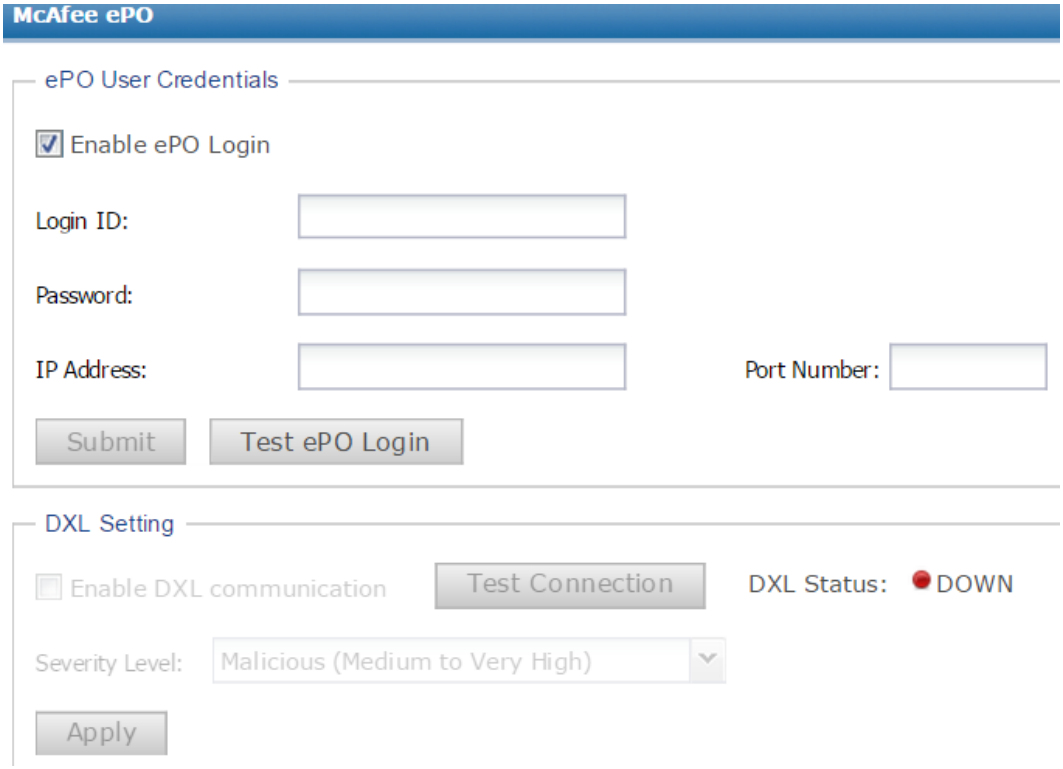
Durch Integration in McAfee ePO kann McAfee ePO Informationen zum auf dem Zielhost installierten Betriebssystem und Browsern sammeln. McAfee Advanced Threat Defense verwendet diese Informationen, um die beste Analyse-VM für die dynamische Analyse auszuwählen.

Vorgehensweise

1 Wählen Sie **Verwalten** | **ePO Login/DXL Setting (ePO-Anmeldung/DXL-Einstellung)**

Die Seite **ePO Login/DXL Setting** (ePO-Anmeldung/DXL-Einstellung) wird angezeigt.

Abbildung 6-4 McAfee ePO-Integration



2 Geben Sie die Details in die entsprechenden Felder ein.

Optionsname	Beschreibung
Anmelde-ID	Geben Sie den McAfee ePO-Anmeldenamen ein, den McAfee Advanced Threat Defense für den Zugriff auf den McAfee ePO-Server verwenden soll. McAfee empfiehlt, ein McAfee ePO-Benutzerkonto mit Leseberechtigung zu erstellen, das für die Integration benötigt wird.
Kennwort	Geben Sie das zur eingegebenen **Anmelde-ID** gehörige Kennwort ein.
IP-Adresse	Geben Sie die IPv4-Adresse des McAfee ePO-Servers ein. Wenden Sie sich an Ihren McAfee ePO-Administrator, um die IP-Adresse zu erhalten.
Portnummer	Legen Sie den HTTPS-Abhörport auf dem McAfee ePO-Server fest, der für die Kommunikation zwischen McAfee Advanced Threat Defense und McAfee ePO verwendet werden soll. Wenden Sie sich an Ihren McAfee ePO-Administrator, um die Portnummer zu erhalten.
Test ePO Login (ePO-Anmeldung testen)	Klicken Sie auf diese Schaltfläche, um zu überprüfen, ob McAfee Advanced Threat Defense den konfigurierten McAfee ePO-Server über den angegebenen Port erreichen kann.
Senden	Klicken Sie auf diese Schaltfläche, um die Konfiguration zu speichern und die Integration von McAfee Advanced Threat Defense inMcAfee ePOzu aktivieren. Stellen Sie sicher, dass die Testverbindung erfolgreich hergestellt werden konnte, bevor Sie auf **Senden** klicken.
Deaktivieren	Klicken Sie darauf, um die Integration von McAfee Advanced Threat Defense in McAfee ePOzu deaktivieren.

Integration in Data Exchange Layer

McAfee Data Exchange Layer (DXL) enthält Client-Software und einen oder mehrere Broker für bidirektionale Kommunikation zwischen Endpunkten in einem Netzwerk. Der McAfee DXL-Client wird auf allen verwalteten Endpunkten installiert, sodass Bedrohungsinformationen unmittelbar mit allen anderen Diensten und Geräten geteilt werden und Bedrohungen sich dadurch nicht mehr einfach ausbreiten können.

Durch die Integration von Advanced Threat Defense in McAfee DXL kann Advanced Threat Defense den Analysebericht der in Advanced Threat Defense analysierten Proben an den McAfee DXL-Broker senden. Die Proben von Advanced Threat Defense werden in einem Thema unter /mcafee/event/atd/file/report auf dem McAfee DXL-Broker veröffentlicht. Clients wie Security Information and Event Management (SIEM), die dieses Thema (/mcafee/event/atd/file/report) abonniert haben, können die Analyseberichte vom McAfee DXL-Broker abrufen, um eine stabile Sicherheitsreputationsdatenbank aufzubauen. Clients mit Abonnements können auf diese Datenbank Bezug nehmen und in ihr Netzwerk eingehende Dateien entsprechend dem Analysebericht der Dateien behandeln.

Im Folgenden wird beschrieben, wie Advanced Threat Defense die Analyseberichte im McAfee DXL-Kanal veröffentlicht:

1 Advanced Threat Defense erhält die Probedateien zur Analyse von verschiedenen Kanälen wie McAfee Network Security Platform, McAfee Web Gateway usw.

2 Die Analyseübersicht wird dann zur weiteren On-Demand-Verteilung für Clients mit Abonnement an den McAfee DXL-Broker gesendet.

Im folgenden Diagramm wird die Integration von Advanced Threat Defense und McAfee DXL beschrieben.

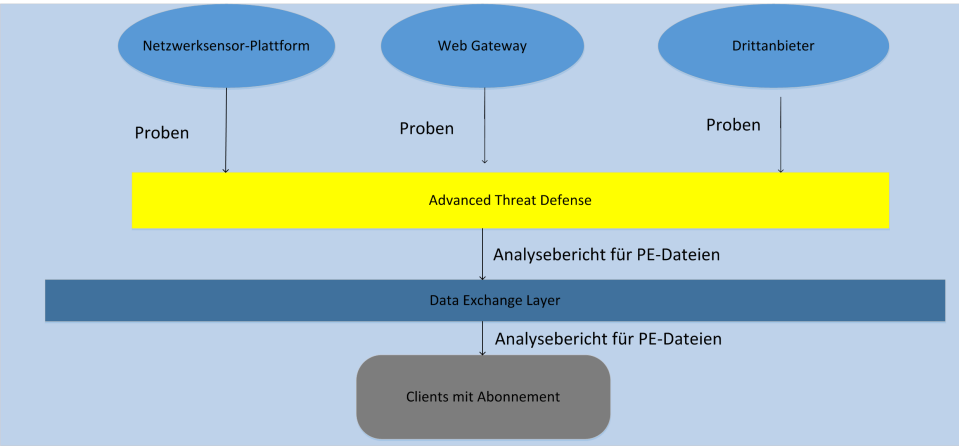
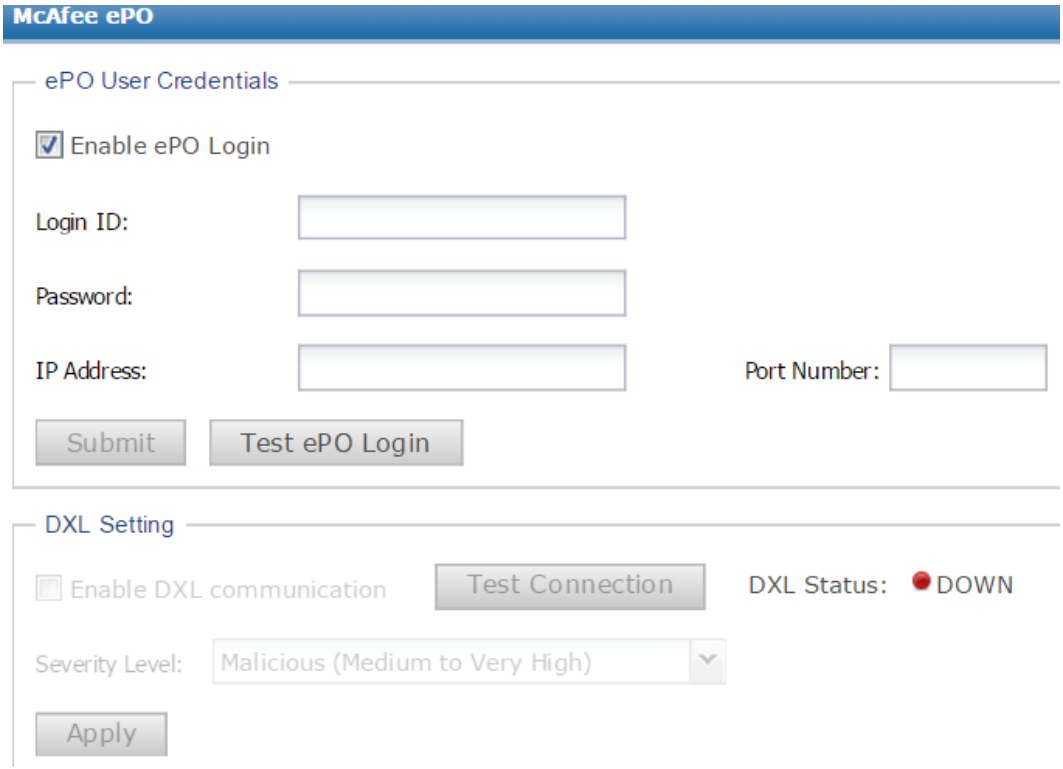


Abbildung 6-5 Advanced Threat Defense – Integration von Data Exchange Layer

Konfigurieren der Data Exchange Layer-Integration

Vorgehensweise

1 Wählen Sie **Verwalten | ePO Login/DXL Setting (ePO-Anmeldung/DXL-Einstellung).** Die Seite **McAfee ePO** wird angezeigt.



2 Geben Sie die Details in die entsprechenden Felder ein. Siehe Konfigurieren der McAfee ePO-Integration auf Seite 258 (Konfigurieren der McAfee ePO-Integration)

3 Klicken Sie auf **Verbindung testen**. Wird die Meldung **Test connection is successful** (Testverbindung erfolgreich) angezeigt, klicken Sie auf **OK**.

4 Gehen Sie im Bereich **DXL Setting** (DXL-Einstellung) wie folgt vor:

- Wählen Sie **Enable DXL communication** (DXL-Kommunikation aktivieren).
- Wählen Sie in der Dropdown-Liste **Schweregrad** den Ihren Anforderungen entsprechenden Schweregrad aus.
- Im Feld **DXL Status** (DXL-Status) wird der DXL-Verbindungsstatus angezeigt.

5 Klicken Sie auf **Übernehmen**. Wird die Meldung **Test DXL connection successful** (DXL-Testverbindung erfolgreich) angezeigt, klicken Sie auf **OK**.

Integration in McAfee Next Generation Firewall

McAfee Next Generation Firewall integriert Sicherheitsfunktionen mit hoher Verfügbarkeit und Verwaltbarkeit. Sie integriert Application Control, Intrusion Prevention System (IPS) und Umgehungsprävention in eine einzige, preiswerte Lösung. Folgende Schritte sollten von McAfee Next Generation Firewall-Kunden durchgeführt werden, um McAfee Next Generation Firewall in McAfee Advanced Threat Defense zu integrieren:

1 Erstellen Sie einen Advanced Threat Defense-Benutzer mit dem Namen "ngfw", nachdem Sie sich als Administrator bei Advanced Threat Defense angemeldet haben. Dieser Benutzer verfügt über dieselben Berechtigungen wie der Benutzer "nsp".

2 Starten Sie amas von der CLI aus neu.

3 Verwenden Sie im SCM den Benutzer "ngfw", um REST-API-Aufrufe auszuführen.



Es werden keine Änderungen am bestehenden SOFA-Protokoll zur Dateiübertragung vorgenommen. Da ein Benutzer mit dem Namen "ngfw" existiert, wird davon ausgegangen, dass alle Datenübertragungen über den SOFA-Kanal von McAfee NGFW-Appliances erfolgen.

Konfigurieren des Proxy-Servers für die Internetverbindung

Advanced Threat Defense stellt für die Internetverbindung Verbindungen zu verschiedenen Proxy-Servern her. Je nach Herkunft des Datenverkehrs ermittelt Advanced Threat Defense den Proxy-Server, über den Internetzugriffsanfragen vom Datenverkehr geleitet werden müssen.

Diese Proxy-Server können in Advanced Threat Defense für die Bearbeitung von Internetzugriffsanfragen konfiguriert werden:

- **GTI HTTP Proxy** – Diese Einstellung ist für die Analyseprofile relevant, bei denen *GTI-Reputation* aktiviert ist. McAfee Advanced Threat Defense sendet eine Anfrage an einen McAfee GTI-Server, um den McAfee GTI-Faktor für die verdächtige Datei abzurufen, die analysiert wird. Wenn das Kundennetzwerk unter dem Proxy geschützt ist, geben Sie die Details des Proxy-Servers hier an, damit die McAfee GTI-Anfragen gesendet werden können.
- **Malware Site Proxy** – Die Einstellung ist anzuwenden, wenn die von Analyse-VMs analysierten Proben Internetzugriff anfordern. Der unter **Malware Site Proxy** angegebene Proxy-Server bearbeitet die Anfrage. Da der Datenverkehr von einer Analyse-VM bösartig sein kann, sollten Sie diesen Datenverkehr eventuell von Ihrem Produktionsnetzwerk trennen.

Aufgaben

- *Angeben von Proxy-Einstellungen für den Datenverkehr von Global Threat Intelligence* auf Seite 262
- *Festlegen der Malware-Website-Proxy-Einstellungen für Malware-Datenverkehr* auf Seite 263

Angeben von Proxy-Einstellungen für den Datenverkehr von Global Threat Intelligence

Vorgehensweise

1 Wählen Sie **Verwalten** | **Proxy-Einstellungen**.

Auf der Seite **Proxy-Einstellungen** wird der Abschnitt **GTI HTTP Proxy** angezeigt.

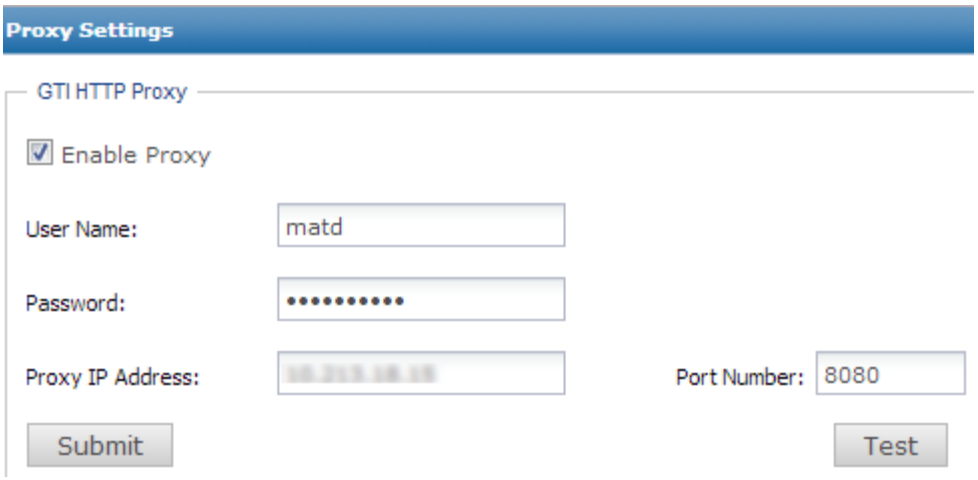


Abbildung 6-6 Seite Proxy-Einstellungen

Zum Aktivieren dieser Option muss die Option **GTI File Reputation** (GTI-Datei-Reputation) unter **Analyze Options** (Analyseoptionen) aktiviert sein.

2 Geben Sie im Bereich **GTI HTTP Proxy** die entsprechenden Informationen in die jeweiligen Felder ein.

Optionsname	Beschreibung
Enable Proxy (Proxy aktivieren)	Wählen Sie die Verbindung von McAfee Advanced Threat Defense mit einem Proxy-Server für den Internetzugriff aus.
Benutzername	Geben Sie den Benutzernamen an, den McAfee Advanced Threat Defense für die Proxy-Internetverbindung verwenden soll.
Kennwort	Geben Sie das entsprechende Kennwort an.
Proxy IP Address (Proxy-IP-Adresse)	Geben Sie die IPv4-Adresse des Proxy-Servers ein.
Portnummer	Geben Sie die Portnummer des Proxy-Servers für eingehende Verbindungen ein.
Testen	Klicken Sie auf diese Schaltfläche, um zu überprüfen, ob McAfee Advanced Threat Defense den konfigurierten HTTP-Proxy-Server über den angegebenen Port erreichen kann.
Senden	Klicken Sie auf diese Schaltfläche, um die Proxy-Einstellungen in der Datenbank zu speichern. Stellen Sie sicher, dass die Testverbindung erfolgreich hergestellt werden konnte, bevor Sie auf **Senden** klicken.

Festlegen der Malware-Website-Proxy-Einstellungen für Malware-Datenverkehr

Vorgehensweise

1 Wählen Sie **Verwalten** | **Proxy-Einstellungen**aus.

Auf der Seite **Proxy-Einstellungen** wird der Abschnitt **Malware Site Proxy** angezeigt.

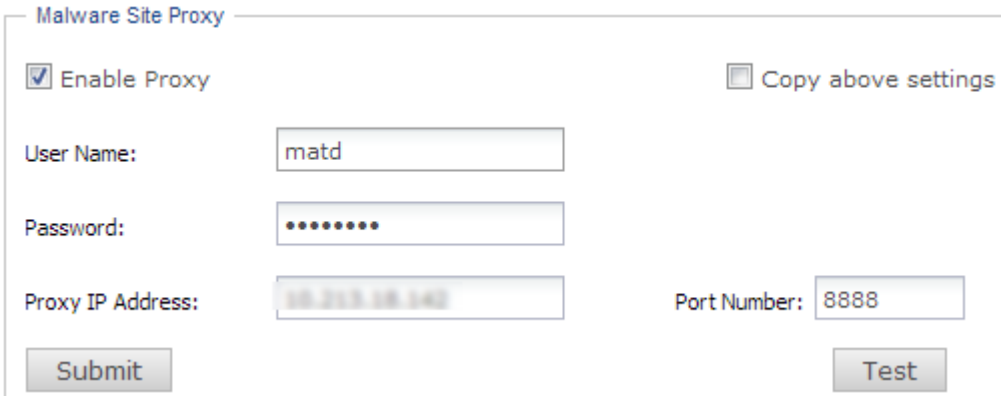


Abbildung 6-7 Seite Proxy-Einstellungen

2 Geben Sie im Bereich "Malware Site Proxy" die entsprechenden Informationen in die jeweiligen Felder ein.

Optionsname	Beschreibung
Enable Proxy (Proxy aktivieren)	Wählen Sie die Verbindung von McAfee Advanced Threat Defense mit einem Proxy-Server für den Internetzugriff aus.
Benutzername	Geben Sie den Benutzernamen an, den McAfee Advanced Threat Defense für die Proxy-Internetverbindung verwenden soll.
Kennwort	Geben Sie das entsprechende Kennwort an.
Proxy IP Address (Proxy-IP-Adresse)	Geben Sie die IPv4-Adresse des Proxy-Servers ein.
Portnummer	Geben Sie die Portnummer des Proxy-Servers für eingehende Verbindungen ein.
Copy above settings (Obige Einstellungen kopieren)	Aktivieren Sie dieses Kontrollkästchen, um die im Abschnitt **GTI HTTP Proxy Settings** (GTI-HTTP-Proxy-Einstellungen) festgelegten Einstellungen zu replizieren.
Testen	Klicken Sie auf diese Schaltfläche, um zu überprüfen, ob McAfee Advanced Threat Defense den konfigurierten HTTP-Proxy-Server über den angegebenen Port erreichen kann.
Senden	Klicken Sie auf diese Schaltfläche, um die Proxy-Einstellungen in der Datenbank zu speichern. Stellen Sie sicher, dass die Testverbindung erfolgreich hergestellt werden konnte, bevor Sie auf **Senden** klicken.

Konfigurieren der Syslog-Einstellung

Mit dem Syslog-Mechanismus werden die Analyseergebnis-Ereignisse über den Syslog-Kanal an Security Information and Event Management (SIEM) wie McAfee Enterprise Security Manager (McAfee ESM) übertragen. Dieser Vorgang betrifft alle Dateien, die von Advanced Threat Defense analysiert werden. Sie können einen externen Syslog-Server konfigurieren, an den folgende Informationen gesendet werden:

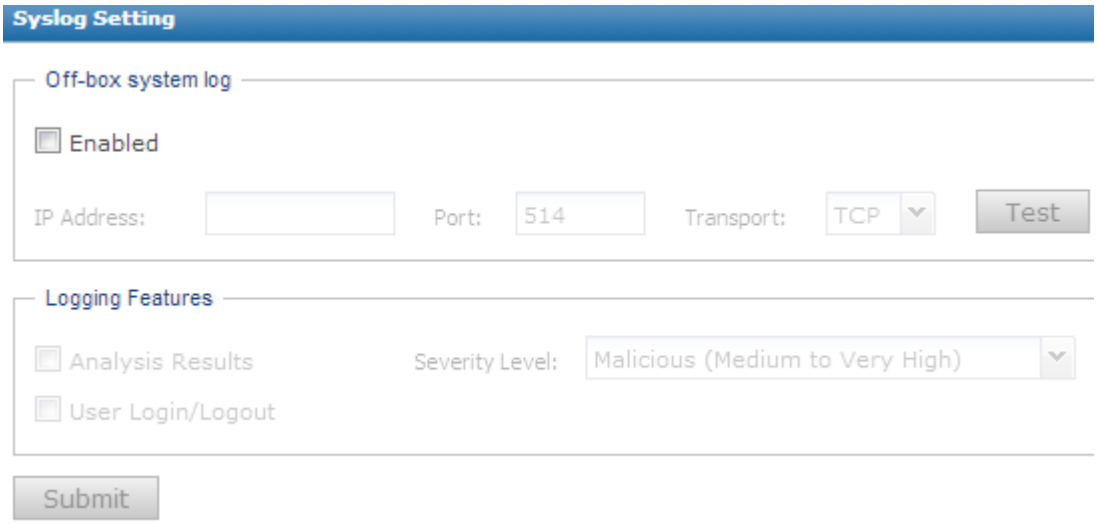
- Analyseergebnisse
- Informationen zu An- und Abmeldungen von Benutzern

Die Analyseergebnisse sowie An- und Abmeldeereignisse werden an den SIEM-Empfänger gesendet. Dort werden die Informationen analysiert und an ESM gesendet. Die Zusammenfassung wird anschließend in der ESM-Benutzeroberfläche angezeigt und kann als Repository für Verlaufsdaten behandelt werden.

Der SIEM-Empfänger und ESM können sich auf unterschiedlichen Appliances oder in der gleichen virtuellen Umgebung befinden

Vorgehensweise

1 Wählen Sie **Verwalten** | **Syslog Setting (Syslog-Einstellung)**.

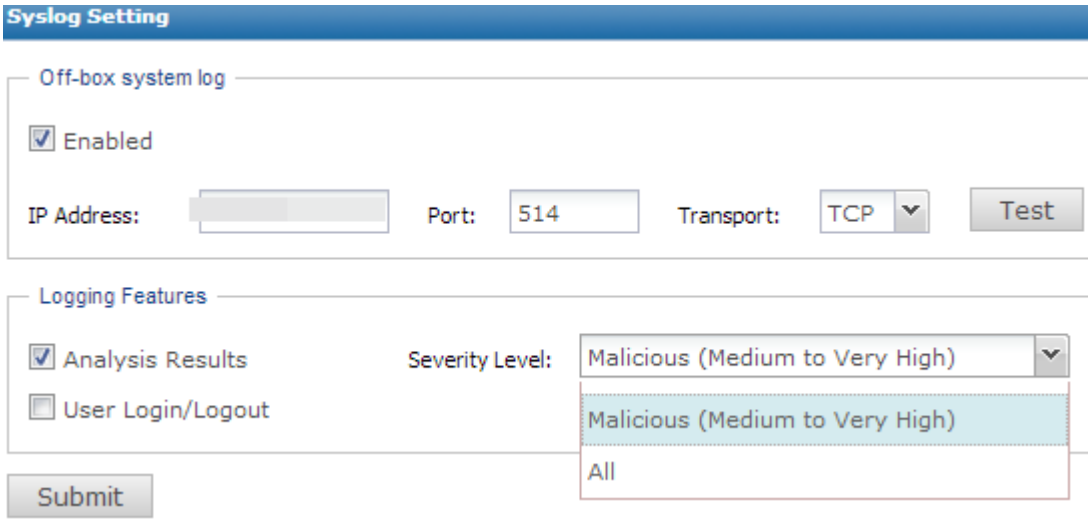


2 Nehmen Sie im Bereich**Off-Box-Systemprotokollierung** folgende Einstellungen und Einträge vor.
   - Wählen Sie **Aktiviert** aus.
   - **IP-Adresse** – IP-Adresse des Syslog-Servers
   - **Port** – Portnummer zum Empfangen für den Syslog-Server (Standardport ist 514)
   - **Transport** – Wählen Sie in der Dropdown-Liste ein Protokoll aus

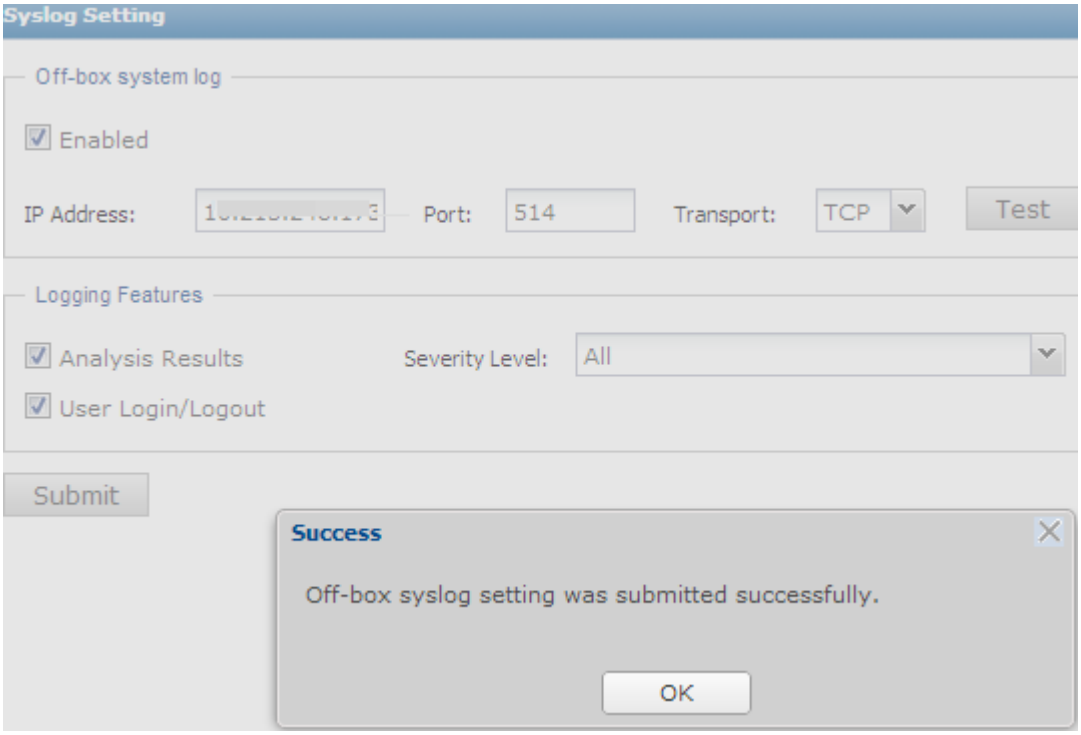
3 Klicken Sie auf **Test**. Wenn gemeldet wird, dass der Vorgang erfolgreich durchgeführt wurde, klicken Sie auf **OK**.

4 Nehmen Sie im Bereich**Logging Features** (Protokollierungsfunktionen) folgende Einstellungen und Einträge vor.

- Wählen Sie **Analysis Results** (Analyseergebnisse).
- Wählen Sie in der Dropdown-Liste **Schweregrad** einen Schweregrad aus.
- Wenn Sie die An- und Abmeldedaten mit einem Zeitstempel speichern möchten, wählen Sie**User Login/Logout** (Benutzeranmeldung/-abmeldung) aus.



5 Klicken Sie auf **Senden**. Die Meldung **Off-box syslog setting was submitted successfully** (Senden der Off-Box-Syslog-Einstellung erfolgreich) wird angezeigt.



Beispiel für Analyseprotokollereignisse, das in ESM angezeigt wird:


```
<182>Aug 19 22:49:05 ATD-3000 ATD2ESM[4278]: {"Summary": { "Event_Type": "ATD File
Report","MISversion": "3.2.2.2.40833","SUMversion": "3.2.2.2.40833","OSversion":
"win7sp1","field": "54fa_00ca_5575b4f8_d5e2_421c_80d0_3daa4d67ff89","Parent MD5":
"Not Available","ATD IP": "10.213.248.14","TaskId": "50128","JobId":
"50127","JSONversion": "1.001.0718","hasDynamicAnalysis": "true","Subject":
{"Name": "v_upx200w.exe","Type": "PE32 executable (console) Intel 80386","md5":
"65B48733E50FD44009C6566B8C1F4393","sha-1":
"F3B0901F44A0079431592011C6757BAC19EEAD3C","size": "19456","Timestamp": "2014-08-19
22:48:28","parent_archive": "Not Available"},"Selectors": [{"Engine":
"CustomYara","MalwareName": "---","Severity": "5"},{"Engine":
"Sandbox","MalwareName": "---","Severity": "5"}],"Verdict": {"Severity":
"5","Description": "Subject is malicious"},"Stats": [{"ID": "0","Category":
"Persistence, Installation Boot Survival","Severity": "5"},{"ID": "1","Category":
"Hiding, Camouflage, Stealthiness, Detection and Removal Protection","Severity":
"1"},{"ID": "2","Category": "Security Solution / Mechanism bypass, termination and
removal, Anti Debugging, VM Detection","Severity": "5"},{"ID": "3","Category":
"Spreading","Severity": "2"},{"ID": "4","Category": "Exploiting,
Shellcode","Severity": "0"},{"ID": "5","Category": "Networking","Severity": "5"},
{"ID": "6","Category": "Data spying, Sniffing, Keylogging, Ebanking
Fraud","Severity": "4"}],"Behavior": [" CUSTOM yara test: create/remove directory
[custom_1]"," CUSTOM yara test: run key, delete value [custom_2]","Created content
under Windows system directory","Deleted AV auto-run registry key","Created a
socket bound to a specific service provider and listen to an open port","Changed
```

```
the protection attribute of the process","Installed low level keyboard hook
procedure","Deleted a key from auto-run registry entry","Altered auto-run registry
entry that executed at next Windows boot"]}}
```

Beispiel für Ereignisse der Benutzeranmeldung/-abmeldung, das in ESM angezeigt wird:

```
<181>Aug 20 00:33:42 ATD-3000 MATD-LOG[6902]: {"Action": "Successful user login",
"User": "meg", "UserID": "5", "Timestamp": "2014-08-20 07:33:42", "Client":
"10.213.248.120"}
```

Konfigurieren von DNS-Einstellungen

Bei der Ausführung senden einige Dateien möglicherweise DNS-Abfragen zur Auflösung von Namen. Meist versuchen Malware-Programme durch solche Abfragen festzustellen, ob sie in einer Sandkastenumgebung ausgeführt werden. Schlägt die DNS-Abfrage fehl, wählt die Datei unter Umständen einen Alternativpfad. Wenn McAfee Advanced Threat Defense eine solche Datei dynamisch analysiert, können Sie einen Proxy-DNS-Dienst verwenden, um das tatsächliche Verhalten der Datei aufzudecken.

Vorgehensweise

1 Wählen Sie **Verwalten** | **DNS Setting (DNS-Einstellung)**.

Die Seite **DNS Setting** (DNS-Einstellung) wird angezeigt.

2 Geben Sie die entsprechenden Informationen in die jeweiligen Felder ein.

Optionsname	Beschreibung
Domain (Domäne)	Geben Sie den Namen für die Active Directory-Domäne an, beispielsweise McAfee.com.
Preferred DNS Server (Bevorzugter DNS-Server)	Geben Sie die IPv4-Adresse des primären DNS-Proxy-Servers an. Die DNS-Abfragen von Analyse-VMs gehen zu diesem DNS-Server.
Alternate DNS Server (Alternativer DNS-Server)	Geben Sie die IPv4-Adresse des sekundären DNS-Proxy-Servers an. Wenn die Analyse-VM den primären DNS-Server nicht erreichen kann, gehen die DNS-Abfragen an den sekundären DNS-Server.
Testen	Klicken Sie auf diese Schaltfläche, um zu überprüfen, ob McAfee Advanced Threat Defense den bevorzugten oder den alternativen DNS-Server erreichen kann.
Submit (Senden)	Klicken Sie auf diese Schaltfläche, um die Konfiguration in der Datenbank zu speichern. Stellen Sie sicher, dass die Testverbindung erfolgreich hergestellt werden konnte, bevor Sie auf **Senden** klicken.

Konfigurieren der Datums- und Uhrzeiteinstellungen

Bevor Sie beginnen

- Sie müssen über *Administratorbenutzer*-Berechtigungen verfügen, um die Einstellungen von Datum und Uhrzeit anzuzeigen oder zu ändern.
- Wenn Sie Domänennamen von Network Security Protocol-Servern verwenden möchten, stellen Sie sicher, dass die DNS-Server in McAfee Advanced Threat Defense ordnungsgemäß konfiguriert sind.

Sie können Datum und Uhrzeit in der McAfee Advanced Threat Defense Appliance Ihren Wünschen entsprechend auf der Seite **Date and Time Settings** (Datums- und Uhrzeiteinstellungen) festlegen. McAfee Advanced Threat Defense verwendet Ihre Einstellungen zu Datum und Uhrzeit für alle Funktions- und Anzeigezwecke. Datum und Uhrzeit der Benutzeroberflächen, Berichte, Protokolldateien und CLI der McAfee Advanced Threat Defense-Web-Anwendung richten sich nach Ihren Einstellungen von Datum und Uhrzeit. Beispielsweise der Zeitstempel der Seiten "Analysis Status" (Analysestatus) und "Analysis Results" (Analyseergebnisse) richtet sich nach dem Datum und der Uhrzeit, das bzw. die Sie konfiguriert haben.

Sie können Datum und Uhrzeit entweder manuell angeben oder die Network Time Protocol-Server (NTP) als Quelle für McAfee Advanced Threat Defense konfigurieren. Sie können bis zu drei Network Time Protocol-Server (NTP-Server) konfigurieren, wenn Sie NTP-Server angeben. McAfee Advanced Threat Defense dient in diesem Fall als NTP-Client und wird mit dem NTP-Server mit der höchsten verfügbaren Priorität synchronisiert.

- Die Synchronisierung mit NTP-Servern ist in McAfee Advanced Threat Defense standardmäßig aktiviert. `pool.ntp.org` ist ebenfalls als Standard-NTP-Server konfiguriert. Die standardmäßig eingestellte Zeitzone ist Pacific Standard Time (UTC-8).
- Wenn Sie ein Upgrade von einer vorhergehenden Version durchführen, ohne die Option **Datenbank zurücksetzen** zu aktivieren, werden die Datums- und Uhrzeiteinstellungen der vorherigen installierten Version übernommen. Wenn Sie ein Upgrade durchführen und die Option **Datenbank zurücksetzen** aktivieren, werden die Standardeinstellungen für Datum und Uhrzeit wie oben beschrieben festgelegt.
- Auf der Seite **Date and Time Settings** (Datums- und Uhrzeiteinstellungen) von McAfee Advanced Threat Defense muss stets mindestens ein gültiger NTP-Server angegeben sein. Sie können die Server, die in McAfee Advanced Threat Defense in der Liste von NTP-Servern angegeben sind, ergänzen, bearbeiten oder löschen.
- Basierend auf dem verfügbaren Zugriff auf McAfee Advanced Threat Defense können Sie öffentliche NTP-Server oder lokale NTP-Server in Ihrem Netzwerk angeben.
- Sie können den Domänennamen oder die IPv4-Adresse von NTP-Servern angeben. Bei Angabe von Domänennamen müssen die DNS-Einstellungen in McAfee Advanced Threat Defense konfiguriert sein.

  Bei Angabe von öffentlichen NTP-Servern wird die Verwendung von Domänennamen statt IP-Adressen empfohlen. Die Domäne eines öffentlichen NTP-Servers wird basierend auf verschiedenen Faktoren möglicherweise in verschiedene IP-Adressen aufgelöst.

- Sowohl bei Aktivierung der Synchronisation mit NTP-Servern als auch bei manueller Einstellung von Datum und Uhrzeit muss die erforderliche Zeitzone auf der Seite **Date and Time Settings** (Datums- und Uhrzeiteinstellungen) ausgewählt werden. Bei Konfiguration eines NTP-Servers berücksichtigt McAfee Advanced Threat Defense ausschließlich das Datum und die Uhrzeit des NTP-Servers. Die Zeitzone basiert allerdings auf den Angaben auf der Seite 'Date and Time Settings' ('Datums- und Uhrzeiteinstellungen').
-
- Das Datum und die Uhrzeit eines McAfee Advanced Threat Defense-Clients wirken sich nicht auf die angezeigten Zeitstempel aus. Die aktuelle Zeiteinstellung der McAfee Advanced Threat Defense Appliance ist beispielsweise 10 Uhr morgens PST (UTC-8). Alle Zeitstempel werden grundsätzlich in PST angezeigt – unabhängig davon, von welcher Zeitzone aus Sie auf die McAfee Advanced Threat Defense Appliance zugreifen. Das heißt also, dass die Zeitstempel nicht basierend auf den Datums- und Uhrzeiteinstellungen des Clients konvertiert werden.

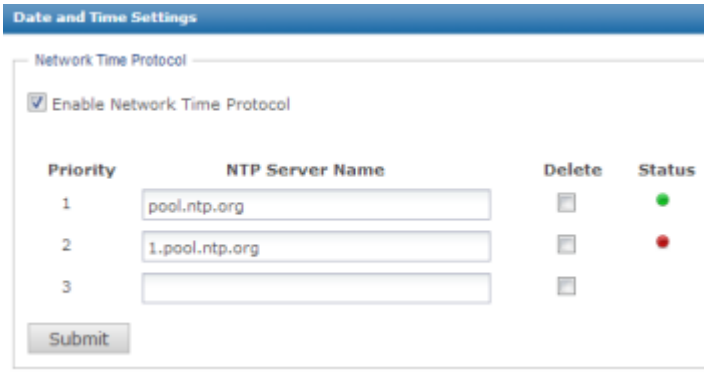
- Wenn die aktuellen Datums- und Uhrzeiteinstellungen geändert werden, wird auch der Zeitstempel von älteren Datensätzen entsprechend geändert. Die aktuelle Zeitzone ist beispielsweise PST (UTC-8), und Sie ändern diese in Japan Standard Time (UTC+9). Daraufhin wird der Zeitstempel aller älteren Datensätze in Japan Standard Time (JST) konvertiert. Der angezeigte Zeitstempel eines Datensatzes auf der Seite **Analysis Status** (Analysestatus) war beispielsweise 01:00 Uhr PST (1 Uhr morgens), bevor die Zeitzone geändert wurde. Nach der Änderung der Zeitzone in JST zeigt der Zeitstempel desselben Datensatzes 18:00 Uhr JST an.
- Die Datums- und Uhrzeiteinstellungen für alle Analyse-VMs werden umgehend mit dem Datum und der Uhrzeit der McAfee Advanced Threat Defense Appliance synchronisiert.

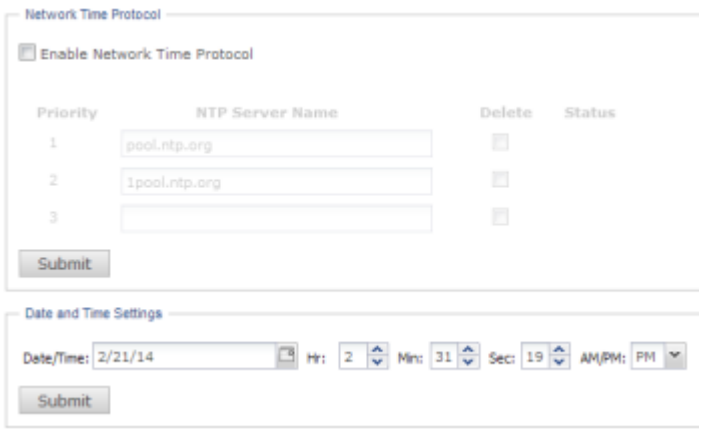
Vorgehensweise

1 Wählen Sie **Verwalten** | **Date and Time Settings (Datums- und Uhrzeiteinstellungen)**

Die Seite **Date and Time Settings** (Datums- und Uhrzeiteinstellungen) wird angezeigt.

2 Geben Sie die entsprechenden Informationen in die jeweiligen Felder ein, und klicken Sie in den erforderlichen Abschnitten einzeln auf **Senden**.

Optionsname	Beschreibung
Enable Network Time Protocol (Network Time Protocol aktivieren)	Aktivieren Sie diese Option, wenn McAfee Advanced Threat Defense als NTP-Client agieren soll. Dies ist standardmäßig ausgewählt. Um die Zeit für McAfee Advanced Threat Defense manuell einzustellen, deaktivieren Sie diese Option.
Priorität	Dies ist die nach Priorität geordnete Reihenfolge für die NTP-Server. In geplanten Intervallen versucht McAfee Advanced Threat Defense eine Synchronisierung mit dem ersten NTP-Server. Wenn dieser nicht verfügbar ist, wird eine Synchronisierung mit dem zweiten und dann mit dem dritten Server angefragt.
NTP Server Name (NTP-Servername)	Geben Sie den Domänennamen oder die IPv4-Adressen der NTP-Server in der nach Priorität geordneten Reihenfolge an, mit denen McAfee Advanced Threat Defense synchronisiert werden soll. Stellen Sie bei der Eingabe von Domänennamen sicher, dass die DNS-Einstellungen ordnungsgemäß konfiguriert wurden. Es muss stets mindestens ein erreichbarer NTP-Server konfiguriert sein.
Löschen	Wählen Sie diese Option aus, wenn Sie einen NTP-Server aus der Liste entfernen möchten.
Status	Gibt an, ob ein bestimmter NTP-Server erreichbar ist. Grün bedeutet, dass der Server erreichbar ist, während Rot keine Erreichbarkeit anzeigt. 

Optionsname	Beschreibung
Datum/Uhrzeit	Um Datum und Uhrzeit für McAfee Advanced Threat Defense manuell anzugeben, deaktivieren Sie die Option **Enable Network Time Protocol** (Network Time Protocol aktivieren), und klicken Sie unter **Network Time Protocol** auf **Senden**. Geben Sie das Datum und die Uhrzeit in den entsprechenden Feldern an, und klicken Sie anschließend unter **Date and Time Settings** (Datums- und Uhrzeiteinstellungen) auf **Senden**. 
Select Time-zone (Zeitzone wählen)	Wählen Sie die erforderliche Zeitzone aus der Liste aus, und klicken Sie unter **Time-zone Setting** (Zeitzoneneinstellung) auf **Senden**. Die standardmäßig eingestellte Zeitzone ist Pacific Time.
Senden	Bei Auswahl dieser Option werden Ihre Änderungen in den entsprechenden Abschnitten der Seite **Date and time settings** (Datums- und Uhrzeiteinstellungen) implementiert und ebenfalls in der Datenbank gespeichert. Wenn Sie für "Network Time Protocol" auf **Senden** klicken, wird eine Erfolgsmeldung angezeigt. Sobald Sie für diese Meldung auf **OK** klicken, überprüft McAfee Advanced Threat Defense, ob die angegebenen NTP-Server erreichbar sind, und aktualisiert für jeden NTP-Server den**Status**.  Sie müssen in allen betreffenden Abschnitten einzeln auf**Senden** klicken. Wenn Sie beispielsweise Änderungen an der NTP-Serverliste vornehmen und außerdem die Zeitzone ändern, müssen Sie sowohl unter **Network Time Protocol** als auch unter **Time-zone Setting** (Zeitzoneneinstellung) auf **Senden** klicken.

Definieren von benutzerdefinierten YARA-Regeln zur Malware-Identifizierung

YARA ist ein regelbasiertes Tool zur Identifizierung und Klassifizierung von Malware. Sie können mithilfe von McAfee Advanced Threat Defense Ihre eigenen YARA-Regeln zur Malware-Identifizierung und -Klassifizierung erstellen. Sie können also Ihre eigenen Malware-Beschreibungen in McAfee Advanced Threat Defense importieren. Darüber hinaus haben Sie die Möglichkeit, mithilfe der

YARA-Regeln die Erkennungsfunktionen von McAfee Advanced Threat Defense ganz nach Ihren Wünschen anzupassen. Sie können beispielsweise YARA-Regeln verwenden, wenn bestimmte Registrierungsvorgänge nicht mit dem von McAfee Advanced Threat Defense zugewiesenen standardmäßigen Schweregrad, sondern mit einem ganz bestimmten Schweregrad gemeldet werden sollen. Sie können YARA-Regeln auch schreiben, um Zero-Day- und Near-Zero-Day-Malware zu erfassen. Sie haben die Möglichkeit, Ihre eigenen YARA-Regeln zu schreiben oder die YARA-Regeln von Dritten zu verwenden.



In diesem Abschnitt bezieht sich das Wort "Probe" sowohl auf Dateien als auch auf URLs, die zur Malware-Analyse an McAfee Advanced Threat Defense gesendet wurden.

Ihre benutzerdefinierten YARA-Regeln können Sie in einer Textdatei speichern. Sie können diese Datei so benennen, dass Sie Änderungen an Ihrem YARA-Regelsatz verfolgen können. Der Import dieser Textdatei in McAfee Advanced Threat Defense erfolgt über die Benutzeroberfläche der Web-Anwendung. Die Regeln werden intern in einer Datei mit dem Namen `custom.yara` gespeichert.

Sofern Sie alle Analyseoptionen für benutzerdefinierte YARA-Regeln aktiviert haben, verarbeitet McAfee Advanced Threat Defense die Probedateien und -URLs in der folgenden Prioritätsreihenfolge:

1. Lokale Whitelist
2. Lokale Blacklist
3. McAfee GTI
4. McAfee Gateway Anti-Malware Engine
5. McAfee Anti-Malware Engine
6. Dynamische Analyse

7 Benutzerdefinierte YARA-Regeln: Hierbei handelt es sich um vom Benutzer erstellte YARA-Regeln.

8 Interne YARA-Regeln: Hierbei handelt es sich um interne YARA-Regeln, die von McAfee definiert und nur bei Bedarf im Zuge eines Software-Upgrades von McAfee Advanced Threat Defense aktualisiert werden. Diese Regeln können Sie nicht anzeigen oder herunterladen.

McAfee Advanced Threat Defense vergleicht die Probe nur mit den YARA-Regeln, wenn sie einer dynamischen Analyse unterzogen wird.

```
rule process_inject
{
meta:
Classification = 32
Description = "Changed access protection of pages to RW/RWE and injected into"
Severity = 4

strings:
$ntget =/(Nt|Zw)GetProcessHeap:/
$ntquery =/(Nt|Zw)QuerySystemInformation(Process|Thread):/
$ntopen =/(Nt|Zw)OpenProcess:/
$ntalloc =/(Nt|Zw)AllocateVirtualMemory:/
$ntwrite =/(Nt|Zw)WriteVirtualMemory:[0-9A-F ]{6,12}\([0-6]{1}[0-9A-E]{2,4},/
$service =/(svchost|csrss|lsass|spoolsv|services|winlogon|explorer|iexplore|winsvc)\.exe/ nocase

condition:
all of them
and
(for any i in (1..#ntquery) : (@ntopen > @ntquery[i])) //sequence of query/open
and
(for any i in (1..#ntopen) : (@service > @ntopen[i])) //service name for NtOpenProcess
}
```

Abbildung 6-8 Beispiel für eine YARA-Regel

Nachdem Sie Ihre YARA-Regeln in McAfee Advanced Threat Defense importiert haben, erfolgt die Malware-Erkennung und -Klassifizierung ebenfalls auf der Grundlage dieser Regeln. Der bei Abschluss der Probenanalyse festgelegte Schweregrad wird als Maximalwert anhand der oben erwähnten Analysemethoden, einschließlich der benutzerdefinierten YARA-Regeln, bestimmt.

Down Selector's Analysis:

Engine	GTI File Reputation	Gateway Anti-Malware	Anti-Malware	Custom Yara	Sandbox	Final
Threat Name	---	---	---	---	---	
Severity	None	None	None	4	2	4

This sample is malicious: final severity level 4

Abbildung 6-9 Von einem benutzerdefinierten YARA-Regelwert beeinflusste Endbewertung

Anmerkungen

- McAfee Advanced Threat Defense unterstützt YARA-Regeln erst ab McAfee Advanced Threat Defense Version 3.2.0.
- McAfee Advanced Threat Defense 3.2.0 unterstützt lediglich YARA-Version 1.0. Entsprechend werden alle im YARA-Benutzerhandbuch der Version 1.0 dokumentierten Funktionen unterstützt.

- Wenn McAfee Advanced Threat Defense als Cluster eingerichtet ist, verwendet jeder Knoten seinen eigenen, separaten Satz von YARA-Regeln. Das bedeutet, dass die von Ihnen im primären Knoten definierten YARA-Regeln nicht automatisch an die sekundären Knoten gesendet werden.
- Die Anzahl der Regeln, die Sie für Ihre benutzerdefinierte YARA-Regeldatei festlegen können, ist unbegrenzt. Ebenfalls gibt es keine Einschränkung hinsichtlich der Dateigröße. Die Anzahl der Regeln und ihre Komplexität kann sich jedoch auf die Leistung von McAfee Advanced Threat Defense auswirken.

Erstellen der benutzerdefinierten YARA-Regeldatei

Bevor Sie beginnen

- Sie sind mit allen Funktionen von YARA vertraut, die McAfee Advanced Threat Defense derzeit unterstützt.
- Sie haben das User API-Protokoll der Probe identifiziert, die Sie als Referenz für die Erstellung Ihrer YARA-Regeln verwenden möchten.

McAfee Advanced Threat Defense wendet die benutzerdefinierten YARA-Regeln auf das User API-Protokoll einer analysierten Probe an. Um benutzerdefinierte YARA-Regeln zu erstellen, die ein bestimmtes Verhalten erfassen, können Sie das User API-Protokoll einer Probe verwenden, die dasselbe Verhalten verursacht hat. Sie können YARA-Regeln verwenden, um Laufzeit-DLLs, Dateivorgänge, Registrierungsvorgänge, Prozessvorgänge und andere im Übersichtsbericht der Analyse gemeldeten Vorgänge für eine Probe zu erfassen. Um beispielsweise eine bestimmte Laufzeit-DLL zu erfassen, prüfen Sie das User API-Protokoll einer Probe, und schreiben Sie eine YARA-Regel für diese DLL.

Vorgehensweise

1 Erstellen Sie eine Textdatei, und öffnen Sie sie in einem Texteditor wie z. B. Windows Editor.

2 Geben Sie die Kommentare in die Textdatei ein, um die APIs oder Daten zu verfolgen, die die Quellen für Ihre YARA-Regeln sind.

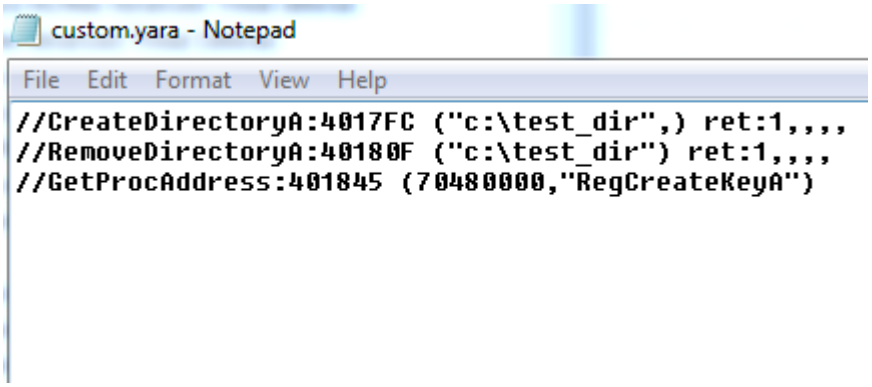


Abbildung 6-10 Kommentare für die benutzerdefinierte YARA-Regeldatei

3 Schreiben Sie die erste Regel, und geben Sie ihr einen Namen.

4 Geben Sie die Metadaten für die Regel ein.

Metadaten sind für Standardregeln obligatorisch und für Hilfsregeln optional. Im Falle von benutzerdefinierten YARA-Regeln können Metadaten eine *Klassifizierung*, eine *Beschreibung* und einen *Schweregrad* enthalten. Verwenden Sie zum Definieren dieser drei Metadatenfelder das

Format: [Name des Metadatenfeldes] = [Zeichenfolge/Wert]. Bei diesen Feldern wird die Groß-/Kleinschreibung nicht beachtet.

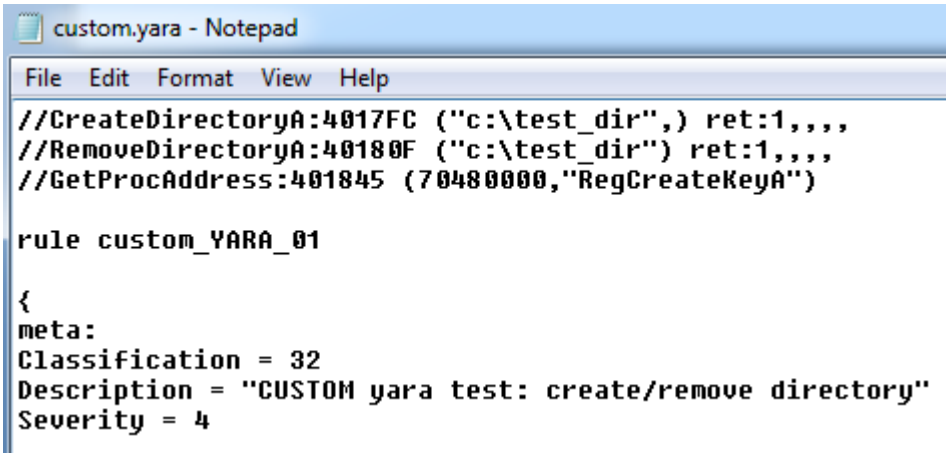


Abbildung 6-11 Metadaten einer benutzerdefinierten YARA-Regel

a Geben Sie optional den Klassifizierungswert für die YARA-Regel ein. Die Klassifizierung meint die Malware-Klassifizierungskategorie, zu der die Verhaltensregel gehört. Verwenden Sie die folgenden Informationen, um den Klassifizierungswert zu berechnen:

Klassifizierung	Wert
Persistence, Installation Boot Survival	1
Hiding, Camouflage, Stealthiness, Detection und Removal Protection	2
Security Solution/Mechanism Bypass, Termination and Removal, Anti Debugging, VM Detection	4
Spreading	8
Exploiting, Shellcode	16
Networking	32
Data Spying, Sniffing, Keylogging, Ebanking Fraud	64

Beispiel: Wenn eine YARA-Regel eine Malware beschreibt, die Spreading (Wert 8), Installation Boot Survival (Wert 1) und Networking (Wert 32) versucht hat, lautet das Klassifizierungsergebnis insgesamt: 8+1+32 = 41.

b Geben Sie die Beschreibung für die Regel ein, die in den Analyseberichten angezeigt wird.

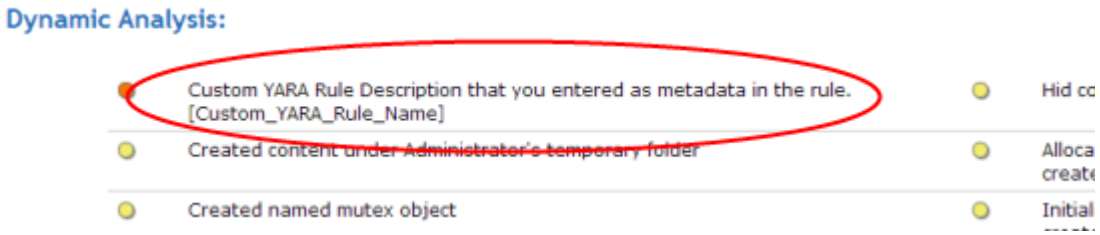

Dynamic Analysis:
Custom YARA Rule Description that you entered as metadata in the rule. [Custom_YARA_Rule_Name]
Created content under Administrator's temporary folder
Created named mutex object

Abbildung 6-12 Name und Beschreibung der benutzerdefinierten YARA-Regel in den Berichten

c Geben Sie einen Schweregrad für das von der YARA-Regel beschriebene Verhalten ein.

Beim Wert des Schweregrads muss es sich um eine ganze Zahl zwischen 1 und 5 handeln, wobei 5 das bösartigste Verhalten angibt. Der Wert des Schweregrads ist für Hilfsregeln irrelevant.

5 Öffnen Sie auf der Seite **Analysis Results** (Analyseergebnisse) das User API-Protokoll der Probe, die Sie als Referenz für die Erstellung Ihrer YARA-Regeln verwenden möchten.

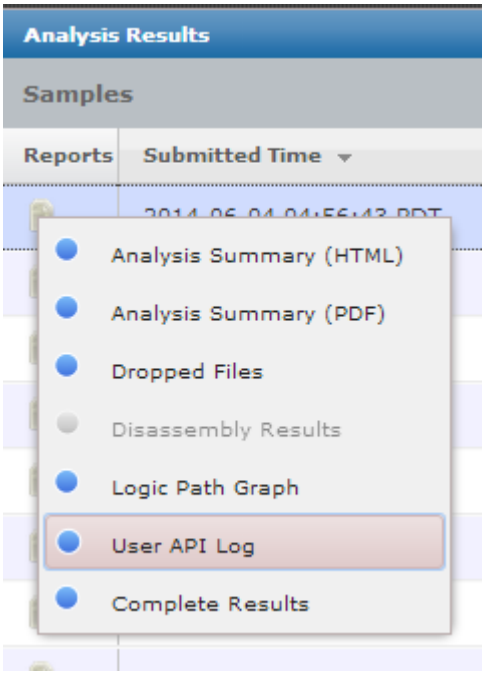


Abbildung 6-13 User API-Protokoll als Referenz für benutzerdefinierte YARA-Regeln

6 Geben Sie die Zeichenfolgen und Bedingungen gemäß der YARA-Syntax ein.

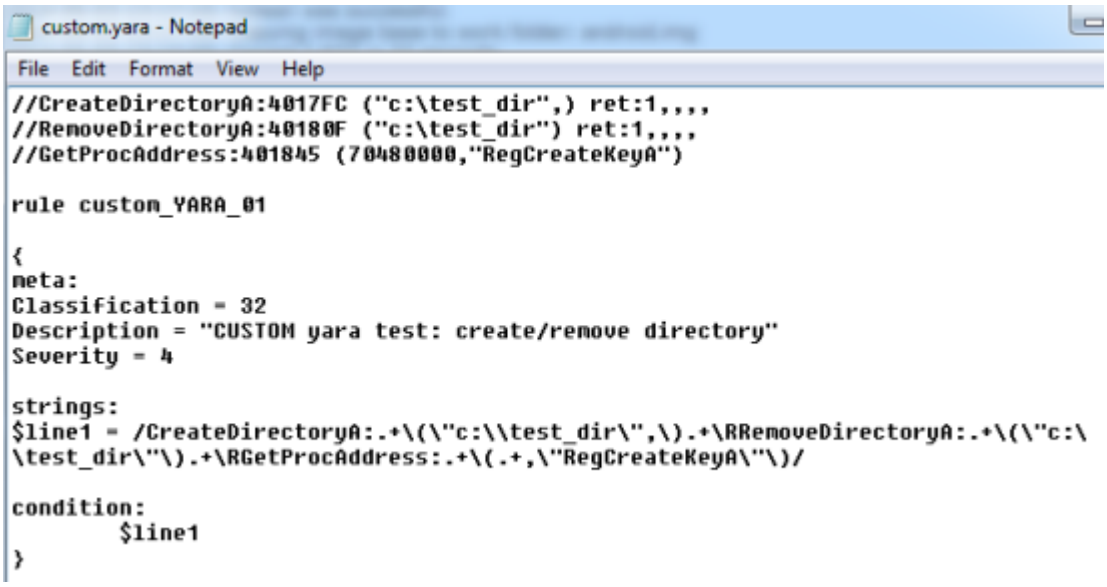


Abbildung 6-14 Benutzerdefinierte YARA-Regel

7 Fügen Sie gemäß der Anforderung der entsprechenden YARA-Textdatei weitere Regeln hinzu, und speichern Sie die Datei anschließend.

Der nächste Schritt ist das Importieren dieser Datei in McAfee Advanced Threat Defense.

Importieren der benutzerdefinierten YARA-Regeldatei

Bevor Sie beginnen

Sie haben Ihre YARA-Regeln, wie unter Erstellen der benutzerdefinierten YARA-Regeldatei auf Seite 274 beschrieben, in einer Textdatei definiert.

Nachdem Sie Ihre YARA-Regeln in einer Textdatei erstellt haben, importieren Sie diese Datei mithilfe der McAfee Advanced Threat Defense-Web-Anwendung in McAfee Advanced Threat Defense. Nach dem Importieren der benutzerdefinierten YARA-Dateien und der Aktivierung der benutzerdefinierten YARA-Regeln nimmt McAfee Advanced Threat Defense diese YARA-Regeln in ihren Mechanismus zur Malware-Erkennung auf.

Vorgehensweise

1 Wählen Sie **Verwalten** | **Custom YARA Rules (Benutzerdefinierte YARA-Regeln)** aus.

2 Aktivieren Sie das Kontrollkästchen **Enable YARA Rules** (YARA-Regeln aktivieren).

Aktivieren Sie das Kontrollkästchen beim Import einer benutzerdefinierten YARA-Textdatei. Bei Bedarf können Sie die benutzerdefinierten YARA-Regeln später deaktivieren.

3 Klicken Sie auf **Durchsuchen**, und suchen Sie die von Ihnen erstellte benutzerdefinierte YARA-Textdatei.

4 Klicken Sie auf **Senden**, um die Datei zu importieren.

Wenn die Datei erfolgreich importiert wurde, wird eine Meldung angezeigt.

Liegen in den YARA-Regeln Syntaxfehler vor, werden die Regeln nicht importiert. Eine Fehlermeldung wird angezeigt. Details zur Art des Fehlers finden Sie im Systemprotokoll. Nehmen wir an, dass in einer regulären Zeichenfolge einer Regel am Ende ein umgekehrter Schrägstrich fehlt. Wenn Sie die benutzerdefinierte YARA-Datei, die diese Regel enthält, importieren, wird eine Fehlermeldung angezeigt.

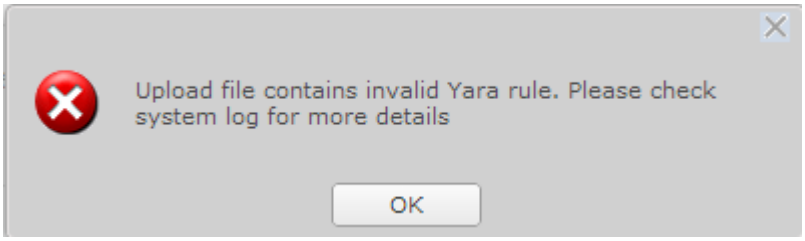


Abbildung 6-15 Meldung, die auf einen Syntaxfehler hinweist

Wählen Sie **Verwalten** | **Systemprotokoll** aus, um das Systemprotokoll zu öffnen, das Details zu den Fehlern enthält.

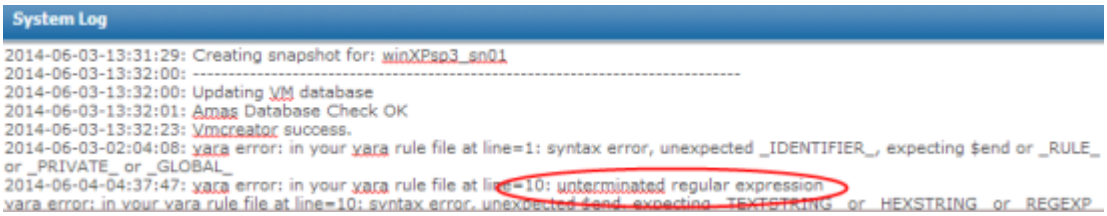

System Log
2014-06-03-13:31:29: Creating snapshot for: winXPsp3_sn01
2014-06-03-13:32:00: ----------
2014-06-03-13:32:00: Updating VM database
2014-06-03-13:32:01: Amas Database Check OK
2014-06-03-13:32:23: Vmcreator success.
2014-06-03-02:04:08: yara error: in your yara rule file at line=1: syntax error, unexpected _IDENTIFIER_, expecting $end or _RULE_ or _PRIVATE_ or _GLOBAL_
2014-06-04-04:37:47: yara error: in your yara rule file at line=10: unterminated regular expression
yara error: in your yara rule file at line=10: syntax error, unexpected $end, expecting _TEXTSTRING_ or _HEXSTRING_ or _REGEXP_

Abbildung 6-16 Details zum Fehler

Aktivieren oder Deaktivieren von YARA-Regeln

Bevor Sie beginnen

Sie haben die benutzerdefinierte YARA-Textdatei in McAfee Advanced Threat Defense importiert.

Nach dem Importieren der benutzerdefinierten YARA-Regeln können Sie sie deaktivieren, wenn Sie sie nicht benötigen. Dies kann beispielsweise bei einer Fehlerbehebung der Fall sein. Wenn Sie die benutzerdefinierten YARA-Regeln deaktivieren, gilt dies für alle von McAfee Advanced Threat Defense analysierten Proben. Sie können die benutzerdefinierten YARA-Regeln zu einem späteren Zeitpunkt wieder aktivieren.

Vorgehensweise

1 Wählen Sie **Verwalten** | **Custom YARA Rules** (Benutzerdefinierte YARA-Regeln) aus.

2 Aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Enable YARA Rules** (YARA-Regeln aktivieren), um benutzerdefinierte YARA-Regeln zu aktivieren bzw. zu deaktivieren.

Wenn Sie die YARA-Regeln aktivieren möchten, die derzeit in der Datenbank von McAfee Advanced Threat Defense vorhanden sind, aktivieren Sie das Kontrollkästchen **Enable YARA Rules**, und klicken Sie auf **Senden**. Das bedeutet, dass Sie die Textdatei für die benutzerdefinierten YARA-Regeln nicht erneut importieren müssen.

Ändern benutzerdefinierter YARA-Regeln

Bevor Sie beginnen

Sie haben die benutzerdefinierte YARA-Textdatei in McAfee Advanced Threat Defense importiert.

Nachdem Sie die benutzerdefinierten YARA-Regeln importiert haben, möchten Sie eventuell einige zusätzliche Regeln hinzufügen oder Änderungen an den bestehenden Regeln vornehmen. Sie könnten beispielsweise den Schweregrad einer Regel ändern.

Vorgehensweise

1 Wählen Sie **Verwalten** | **Custom YARA Rules (Benutzerdefinierte YARA-Regeln) aus**.

2 Klicken Sie auf **Download YARA Rule File** (YARA-Regeldatei herunterladen), um die Datei `custom.yara` aus der McAfee Advanced Threat Defense-Datenbank auf Ihren Client herunterzuladen.

Der Zeitstempel des letzten Imports der Datei `custom.yara` in McAfee Advanced Threat Defense wird Ihnen zu Informationszwecken bereitgestellt.

3 Öffnen Sie die von Ihnen heruntergeladene `custom.yara`-Datei in einem Texteditor und nehmen Sie die erforderlichen Änderungen vor. Sie können z. B. neue Regeln hinzufügen und bestehende Regeln löschen oder ändern. Speichern Sie die Datei, wenn Sie damit fertig sind.

Sie können die Datei gemäß Ihren Anforderungen umbenennen.

4 Importieren Sie die Datei mit den geänderten benutzerdefinierten YARA-Regeln in McAfee Advanced Threat Defense.

Siehe Importieren der benutzerdefinierten YARA-Regeldatei auf Seite 277.

7

Analysieren von Malware

Nach der Konfigurierung von McAfee Advanced Threat Defense können Sie Dateien und Uniform Resource Locators (URLs) zur Analyse hochladen. Sie können den Status der Malware-Analyse über die McAfee Advanced Threat Defense-Web-Anwendung überwachen und dann die Ergebnisse anzeigen.

Inhalt

- *Analysieren von Dateien*
- *Analysieren von URLs*
- *Konfigurieren der Seite "Analysis Status" (Analysestatus)*
- *Anzeigen der Analyseergebnisse*
- *Arbeiten mit dem McAfee Advanced Threat Defense-Dashboard*

Analysieren von Dateien

- Für die Dateiübermittlung können Sie folgende Methoden verwenden:
  - Laden Sie die Datei manuell über die McAfee Advanced Threat Defense-Web-Anwendung hoch.
  - Veröffentlichen Sie die Datei auf dem FTP-Server, der auf der McAfee Advanced Threat Defense Appliance gehostet wird.
  - Verwenden Sie die REST-APIs der McAfee Advanced Threat Defense-Web-Anwendung zum Hochladen der Datei. Siehe *McAfee Advanced Threat Defense RESTful APIs Reference Guide* (Referenzhandbuch zu McAfee Advanced Threat Defense-REST-APIs).
  - Integrieren Sie McAfee Advanced Threat Defense in Network Security Platform und McAfee Web Gateway. Dann senden diese Anwendungen Proben automatisch an McAfee Advanced Threat Defense. Weitere Informationen finden Sie in der entsprechenden Dokumentation.
- Bei Verwendung der McAfee Advanced Threat Defense-Web-Anwendung, der Rest-APIs oder McAfee Web Gateway werden Dateien mit einer Größe von bis zu 128 MB unterstützt. Bei komprimierten Dateien und APK-Dateien beträgt die maximal unterstützte Dateigröße 25 MB.
- Bei Verwendung von Network Security Platform werden Dateien mit einer Größe von bis zu 25 MB unterstützt.

- Bei Dateinamen von Proben unterstützt McAfee Advanced Threat Defense Unicode. Dateinamen können also Zeichen enthalten, die nicht zum englischen Zeichensatz gehören, sowie einige Sonderzeichen außer \'"` <>|; ()[]*?#$&:
- Die Länge des Dateinamens kann bis zu 200 Byte umfassen.

Tabelle 7-1 Unterstützte Dateitypen

Dateitypen	Statische Analyse	Dynamische Analyse
Portierbare ausführbare 32-Bit-Dateien (PE-Dateien)	(.exe, .dll, .scr, .ocx, .sys, .com, .drv, .cpl)	(.exe, .dll, .scr, .ocx, .sys, .com, .drv,
Microsoft Office-Suite-Dokumente	(.doc, .docx, .xls, .xlsx .ppt, .pptx, .rtf)	(.doc, .docx, .xls, .xlsx .ppt, .pptx, .r
Adobe	PDF-Dateien, Adobe Flash-Dateien (SWF)	PDF-Dateien, Adobe Flash-Dateien (S
Komprimierte Dateien (maximal unterstützte Dateigröße: 25 MB)	(.zip, .rar)	(.zip)
Android-Anwendungspakete	(.apk)	(.apk)
Java	Java-Archive (JAR), CLASS	Java-Archive (JAR), CLASS
Bilddateien	(JPEG, PNG, GIF)	Nicht unterstützt

Hochladen von Dateien zur Analyse mittels McAfee Advanced Threat Defense-Web-Anwendung

Bevor Sie beginnen

Das erforderliche Analyseprofil ist verfügbar.

Wenn Sie mithilfe der McAfee Advanced Threat Defense-Web-Anwendung Dateien zur Analyse hochladen, müssen Sie ein Analyseprofil auswählen. Dieses Analyseprofil setzt das mit Ihrem Benutzerkonto verknüpfte Standard-Analyseprofil außer Kraft.

Vorgehensweise

1 Wählen Sie **Analyse** | **Manual Upload (Manuelles Hochladen)** aus.

2 Auf der Seite **Manual Upload** (Manuelles Hochladen) legen Sie die Details gemäß Ihren Anforderungen fest.

Tabelle 7-2 Optionsbeschreibungen

Option	Beschreibung
Datei	Ziehen Sie entweder die Malware-Datei aus dem Windows Explorer und legen Sie sie ab, oder klicken Sie zum Auswählen der Datei auf **Browse** (Durchsuchen). Falls Sie mehrere Dateien senden möchten, laden Sie diese als ZIP-Datei hoch. • Wenn Sie eine mit einem Kennwort geschützte ZIP-Datei hochladen, vergewissern Sie sich, dass Sie das Kennwort im gewünschten Analyseprofil angegeben haben. • Sollte eine dynamische Analyse erforderlich sein, werden die Dateien in der ZIP-Datei auf verschiedenen Instanzen der Analyse-VM ausgeführt. Wenn nicht genügend Analyse-VMs zur Verfügung stehen, bleiben einige Dateien in der Warteschlange, bis wieder Analyse-VMs verfügbar sind. • Da die Dateien in der ZIP-Datei separat analysiert werden, werden für jede Datei separate Berichte erstellt. • Bei Dateinamen von Proben unterstützt McAfee Advanced Threat Defense Unicode. Dateinamen können also Zeichen enthalten, die nicht zum englischen Zeichensatz gehören, sowie einige Sonderzeichen außer \'"` <>|; ()[]*?#$&: • Die Länge des Dateinamens kann bis zu 200 Byte umfassen.
Analyseprofil	Wählen Sie das für die Probe erforderliche Analyseprofil.
Erweitert	Klicken Sie zum Festlegen zusätzlicher Parameter für die Analyse der Probe. Die Optionen unter **Erweitert** stehen nur zur Verfügung, wenn Sie die Datei manuell mittels McAfee Advanced Threat Defense-Web-Anwendung senden. • **User Interactive Mode (Interaktiver Benutzermodus):** Manche Malware erfordert nach der Ausführung eine Benutzereingabe. Dadurch wird in der Regel überprüft, ob die Malware in einem Sandkasten analysiert wird. Falls keine Benutzereingabe erfolgt, wählt die Malware möglicherweise einen anderen Ausführungspfad oder hält die Ausführung sogar an. Bei Auswahl dieser Option können Sie auf die tatsächliche Analyse-VM zugreifen, auf der die Malware ausgeführt wird, und so die Benutzereingabe durchführen. Siehe Hochladen von URLs zur Analyse im interaktiven Benutzermodus auf Seite 281. Nachdem Sie die gewünschten Optionen ausgewählt haben, klicken Sie auf **OK**.
Senden	Klicken Sie zum Hochladen der Datei zur Analyse in McAfee Advanced Threat Defense auf diese Schaltfläche.

Aufgaben

- *Hochladen von URLs zur Analyse im interaktiven Benutzermodus* auf Seite 281

Hochladen von URLs zur Analyse im interaktiven Benutzermodus

Bevor Sie beginnen

Für das erforderliche Analyseprofil wurden die Internetzugriffsoptionen "Sandbox" (Sandkasten) und "Malware" ausgewählt.

Einige Malware kann ggf. nur mit Benutzereingriff ausgeführt werden. Beispiel: Eine Standardeinstellung in der Analyse-VM kann die Ausführung anhalten, bis die Einstellung manuell überschrieben wird. Einige Dateien zeigen möglicherweise Dialogfelder an, in denen Sie eine Auswahl treffen oder eine Bestätigung vornehmen müssen. Durch solches Verhalten versuchen Malware-Programme festzustellen, ob sie in einer Sandkastenumgebung ausgeführt werden. Das

Verhalten von Malware kann gemäß Ihrer Reaktion variieren. Wenn Sie im interaktiven Benutzermodus Dateien senden, wird die Analyse-VM in einem Popupfenster auf Ihrem Client-Computer geöffnet, sodass Sie bei Aufforderung Ihre Eingabe machen können.

Sie können Dateien hochladen, damit sie im interaktiven Benutzermodus ausgeführt werden. Diese Option ist nur verfügbar, wenn Sie eine Datei manuell über die McAfee Advanced Threat Defense-Web-Anwendung hochladen. Bei Dateien, die auf anderem Weg gesendet werden, wie über FTP-Upload oder über Network Security Platform, werden Malware-Anfragen zu Benutzereingriffen ignoriert. Die Screenshots aller Anforderungen sind jedoch im Abschnitt **Screenshots** des Berichts **Analysis Summary** (Analyseübersicht) verfügbar. Sie können dann diese Dateien manuell im interaktiven Benutzermodus erneut senden, um das tatsächliche Verhalten der Datei zu ermitteln.

Da die Analyse-VM in einem Pop-Up geöffnet wird, muss der Popupblocker in Ihrem Browser deaktiviert sein.

Vorgehensweise

1 Wählen Sie **Analyse** | **Manual Upload (Manuelles Hochladen)** aus.

2 Klicken Sie im Feld **File** (Datei) auf **Browse** (Durchsuchen), und wählen Sie die Datei, die Sie zur Analyse senden möchten. Alternativ können Sie die Datei in das angegebene Feld ziehen und dort ablegen.

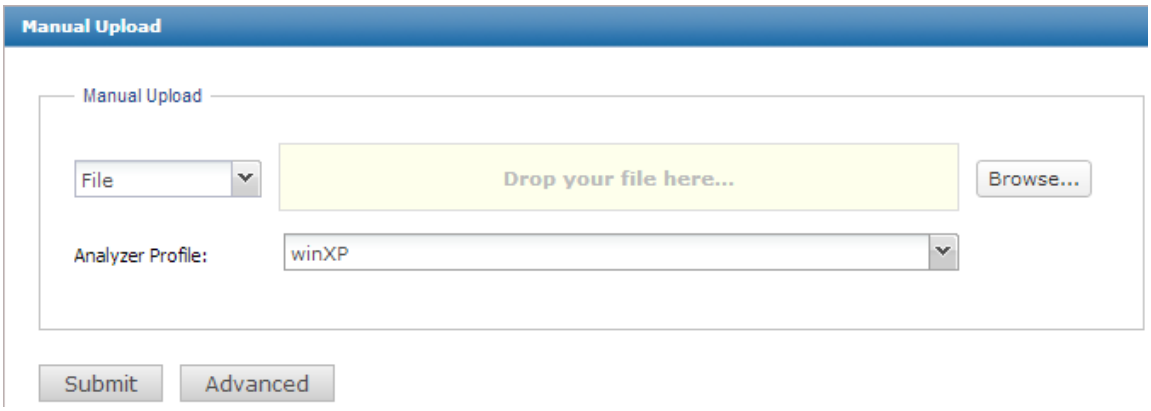


Abbildung 7-1 Senden der Datei

3 Wählen Sie im Feld **Analyzer Profile** (Analyseprofil) das gewünschte Analyseprofil aus der Dropdown-Liste.

4 Klicken Sie auf **Advanced** (Erweitert), und wählen Sie **User Interactive Mode (XMode)** (Interaktiver Benutzermodus (XMode)) aus.

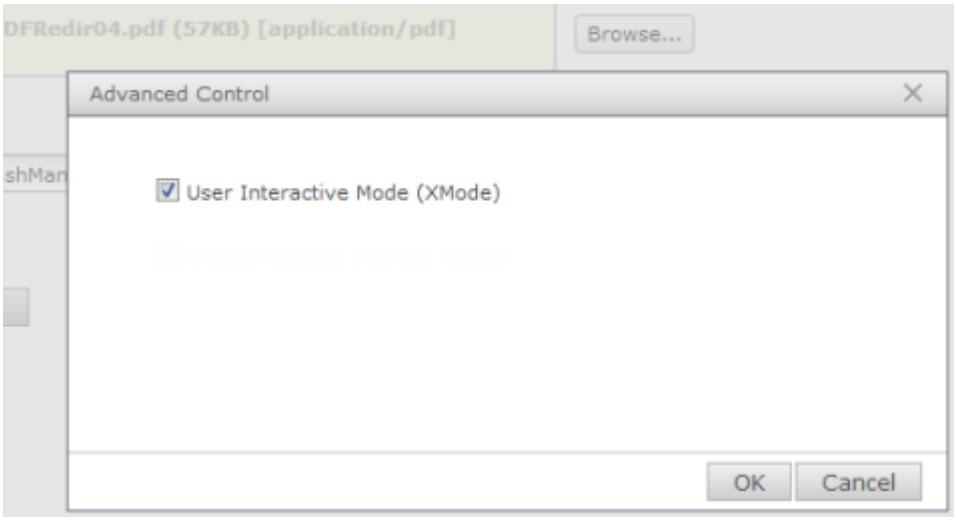


Abbildung 7-2 Auswählen des interaktiven Benutzermodus (User Interactive Mode (XMode))

5 Klicken Sie auf **OK** und dann auf **Submit** (Senden).

Die Probe wird in McAfee Advanced Threat Defense hochgeladen, und eine Erfolgsmeldung mit den Details wird angezeigt.

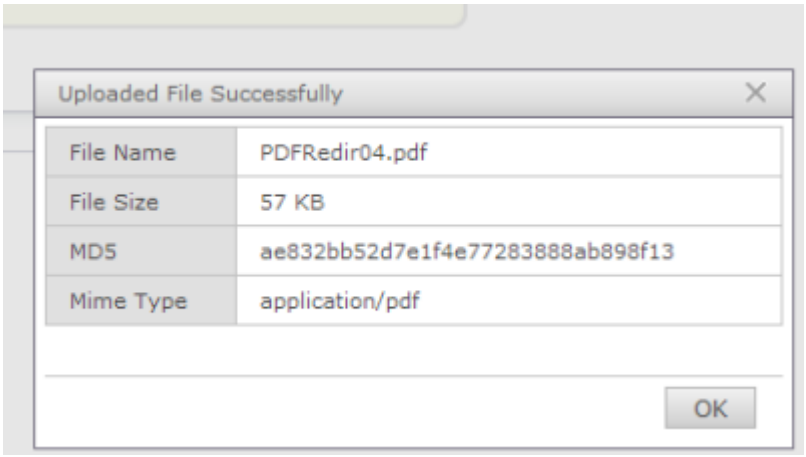


Abbildung 7-3 Meldung zu erfolgreichem Hochladen der Datei

6 Klicken Sie im Dialogfeld **File successfully uploaded** (Datei erfolgreich hochgeladen) auf **OK**.

7 Sie müssen zur Seite **Analysis Status** (Analysestatus) wechseln, um mit der Probe zu interagieren. Klicken Sie daher im Meldungsfeld **User Interactive Mode** (Interaktiver Benutzermodus) auf **OK**, und wählen Sie **Analyse** | **Analysis Status (Analysestatus)** aus.

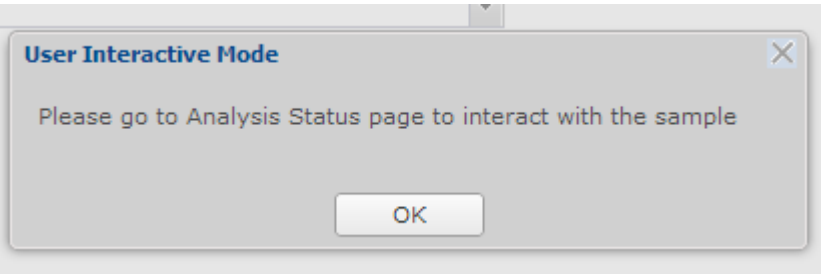


Abbildung 7-4 Meldung "User Interactive Mode" (Interaktiver Benutzermodus)

Auf der Seite **Analysis Status** (Analysestatus) wird die Schaltfläche **X-Mode** in der Spalte **Status** für den entsprechenden Datensatz angezeigt.

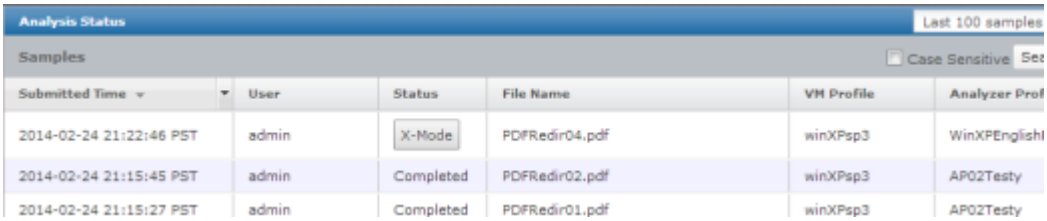


Abbildung 7-5 "X-Mode" auf der Seite "Analysis Status" (Analysestatus)

8 Klicken Sie auf der Seite **Analysis Status** (Analysestatus) für den entsprechenden Datensatz auf **X-Mode**.

Ein Popupfenster wird auf Ihrem Computer angezeigt. Je nach Ihren Browser- und Java-Einstellungen können Sicherheitswarnungen angezeigt werden. Nach dem Bestätigen der

Sicherheitswarnungen wird in einem Popupfenster die Analyse-VM mit den von der Probe geöffneten Dialogfeldern angezeigt. Für die Eingabe können Sie Maus und Tastatur verwenden.

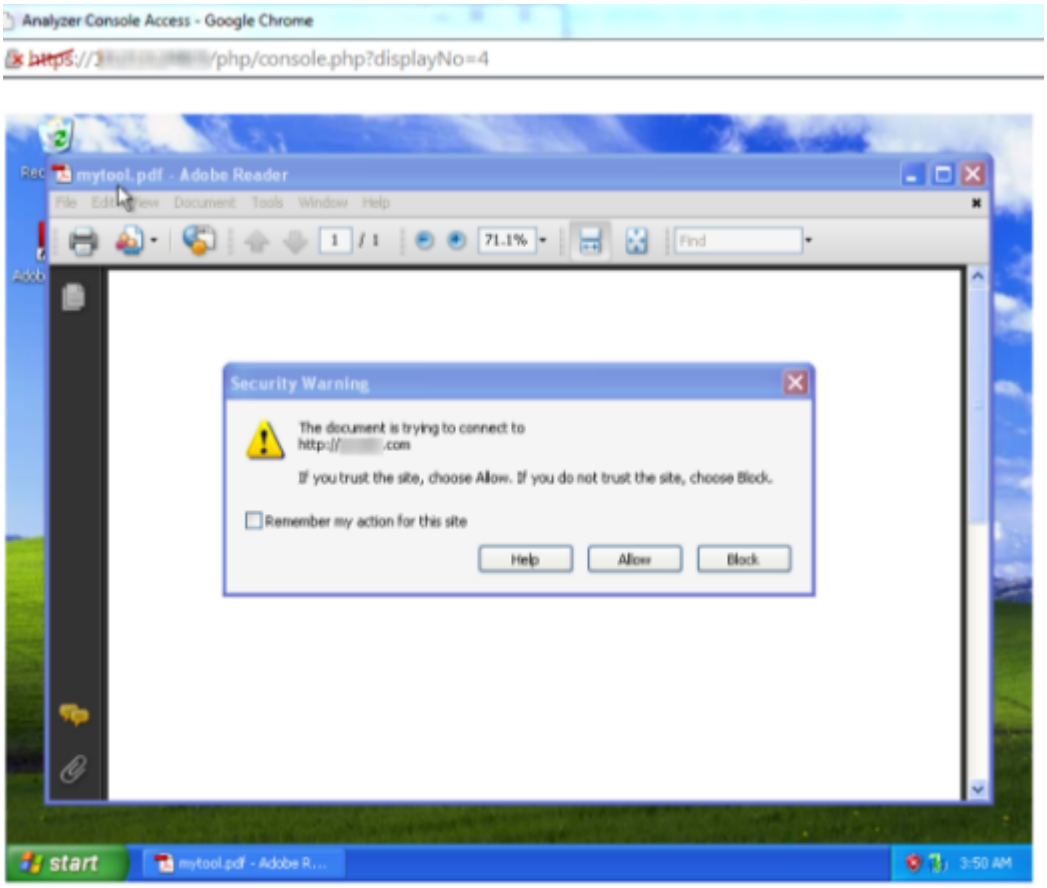


Abbildung 7-6 Zugriff auf die Analyse-VM über ein Popupfenster

Die Ausführung der Datei beginnt, sobald Sie diese gesendet haben, und nicht erst beim Öffnen der Analyse-VM. Bei einigen Meldungen kann es im Hintergrund zu einer Zeitüberschreitung kommen. Wenn Sie die vollständige Ausführung anzeigen möchten, müssen Sie auf der Seite **Analysis Status** (Analysestatus) ohne Verzögerung auf **X-Mode** klicken.

Nachdem die Dateiausführung abgeschlossen ist, meldet sich die Analyse-VM automatisch ab, und Sie können das Pop-Up schließen.

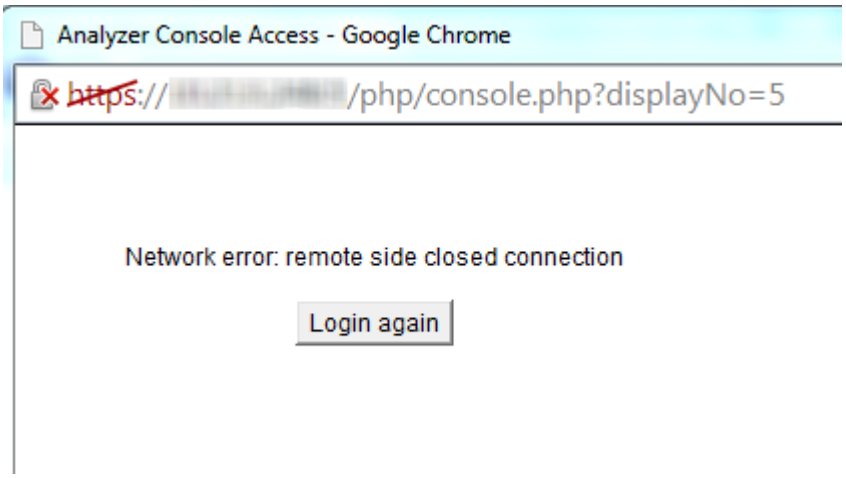


Abbildung 7-7 Analyse-VM meldet sich ab

Hochladen von Dateien zur Analyse über SFTP

Bevor Sie beginnen

- Ihr Benutzername verfügt über die Berechtigung **FTP Access** (FTP-Zugang). Dies ist erforderlich, um auf den auf McAfee Advanced Threat Defense gehosteten FTP-Server zuzugreifen.
- Sie haben das erforderliche Analyseprofil erstellt, das Sie verwenden möchten.
- Sie haben einen FTP-Client auf Ihrem Computer installiert.

Mit SFTP können Sie die unterstützten Dateitypen auf den FTP-Server auf McAfee Advanced Threat Defense hochladen.

FTP ist standardmäßig kein unterstütztes Protokoll für das Hochladen von Proben. Um FTP zum Hochladen von Dateien verwenden zu können, müssen Sie es mit dem CLI-Befehl `set ftp` aktivieren. Siehe set ftp auf Seite 364.

Vorgehensweise

1 Öffnen Sie Ihren FTP-Client, und stellen Sie eine Verbindung mit McAfee Advanced Threat Defense unter Verwendung der folgenden Informationen her.
   - Host – Geben Sie die IP-Adresse von McAfee Advanced Threat Defense ein.
   - User Name – Geben Sie Ihren McAfee Advanced Threat Defense-Benutzernamen ein.
   - Password – Geben Sie Ihr McAfee Advanced Threat Defense-Kennwort ein.
   - Port – Geben Sie 22 ein, den Standardport für SFTP. Für FTP geben Sie 21 ein.

2 Laden Sie die Dateien von der lokalen Site auf die Remote-Site hoch, die sich auf McAfee Advanced Threat Defense befindet.

3 Wählen Sie in der McAfee Advanced Threat Defense-Web-Anwendung **Analyse** | **Analysis Status (Analysestatus)** zum Überwachen des Status der hochgeladenen Dateien.

Analysieren von URLs

Ähnlich dem Senden einer Datei kann in dieser Version auch eine URL an Advanced Threat Defense zur Analyse übermittelt werden. Advanced Threat Defense analysiert die URL in einer Analyse-VM, die durch das Benutzerprofil festgelegt wird, und meldet die Ergebnisse der Dateianalyse. Advanced Threat Defense verwendet nur die lokale Blacklist und die dynamische Analyse für die heruntergeladene Datei. Außerdem wird die McAfee GTI-Reputation der URL gemeldet. Auch das Verhalten des Browsers beim Öffnen einer URL wird hinsichtlich bösartiger Aktivitäten analysiert.

Gehen Sie zum Senden von URLs wie folgt vor:

- Laden Sie die URL manuell über die Advanced Threat Defense-Web-Anwendung hoch.
- Verwenden Sie die REST-APIs der Advanced Threat Defense-Web-Anwendung zum Hochladen der URLs. Siehe *Advanced Threat Defense RESTful APIs Reference Guide* (Referenzhandbuch zu Advanced Threat Defense-REST-APIs).

Bösartige Websites enthalten üblicherweise mehrere Typen von Malware. Wenn ein Benutzer die Website öffnet, wird diejenige Malware heruntergeladen, die die entsprechenden Schwachstellen des Endgeräts angreifen kann. Sie können mehrere Analyse-VMs mit jeweils unterschiedlichen Betriebssystemen, Browsern, Anwendungen und Browser-Plug-Ins erstellen, die für Ihr Netzwerk erforderlich sind. Außerdem können Sie bei Browsern und Betriebssystemen ohne Patch möglicherweise das tatsächliche Verhalten von Websites analysieren.

Der Vorteil von Advanced Threat Defense besteht in einem detaillierten Bericht über zuvor unbekannte bösartige Domänen, Websites und IP-Adressen sowie über das aktuelle Verhalten bereits bekannter bösartiger Domänen, Websites und IP-Adressen. Sie können zudem einen detaillierten Analysebericht über ungefährliche Websites erhalten, die vor Kurzem infiziert wurden.

Advanced Threat Defense analysiert keine URLs, die in Dateien enthalten sind, die zur Analyse eingereicht wurden. Wenn ein Network Security Sensor beispielsweise eine Microsoft Word-Datei sendet, analysiert Advanced Threat Defense die Datei hinsichtlich Malware, analysiert jedoch keine der darin enthaltenen URLs.

Wie analysiert Advanced Threat Defense URLs?

Wählen Sie zum Analysieren von URLs ein Analyseprofil aus, für das der Zugriff sowohl auf den Sandkasten als auch auf das Internet aktiviert ist. Im Folgenden finden Sie den Prozessablauf für den Fall, dass Sie eine URL zur Analyse an Advanced Threat Defense senden:

1 Advanced Threat Defense wendet eine proprietäre Vorgehensweise für die Berechnung des MD5-Hashwerts der URL an. Anschließend gleicht sie diesen MD5-Wert mit seiner lokalen Blacklist ab.



Die lokale Whitelist ist nicht anwendbar für URLs.

2 Es wird angenommen, dass die Datei, auf die sich die URL bezieht, in einem unterstützten Dateityp vorliegt. Anschließend analysiert Advanced Threat Defense die Datei dynamisch mithilfe der entsprechenden Analyse-VM. Es wird angenommen, dass der MD5-Wert der URL nicht in der Blacklist enthalten ist oder die Option **Run All Selected** (Gesamte Auswahl ausführen) im entsprechenden Analyseprofil ausgewählt ist.



Für URLs sind die Analyseoptionen "GTI-Datei-Reputation", "Malware-Schutz" und "Gateway Anti-Malware" irrelevant.

3 Die dynamische Analyse und die Berichterstellung für URLs erfolgen ähnlich der für Dateien. Dabei werden alle Aktivitäten der Analyse-VM, einschließlich Registrierungs-, Prozess-, Datei- und Netzwerkvorgängen sowie Laufzeit-DLLs, erfasst. Wenn die Webseite Dropper-Dateien herunterlädt, analysiert Advanced Threat Defense diese Dateien ebenfalls. Die Ergebnisse dieser Analyse werden in demselben Bericht im Abschnitt zu den eingebetteten/betroffenen Inhalten festgehalten.

4 Stellt eine betroffene Datei eine Verbindung zu anderen URLs her, werden diese mithilfe von TrustedSource auf ihre URL-Reputation und -Kategorisierung untersucht.

Bei der URL-Analyse werden nur HTTP-, HTTPS- und FTP-Protokolle unterstützt.

Hochladen von URLs zur Analyse mittels Advanced Threat Defense-Web-Anwendung

Bevor Sie beginnen

Stellen Sie sicher, dass für das erforderliche Analyseprofil die Internetzugriffsoptionen "Sandbox" (Sandkasten) und "Malware" ausgewählt wurden.

Abhängig von den Anforderungen können Sie die URLs mit zwei verschiedenen Optionen hochladen. Verwenden sie hierzu die Advanced Threat Defense-Web-Anwendung.

Folgende Optionen sind für das manuelle Hochladen von URLs verfügbar:

- **URL** – Die ausgewählte URL wird an die Analyse-VM gesendet, und die Datei, auf die die URL verweist, wird zur Analyse auf die Analyse-VM heruntergeladen. Beispiel: Übermittelt ein Benutzer die URL "http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe", wird die URL an die Analyse-VM gesendet, und anschließend wird die Datei "putty.exe" auf die Analyse-VM heruntergeladen.
- **URL Download** – Die ausgewählte URL wird auf die Advanced Threat Defense Appliance heruntergeladen und anschließend zur Analyse an die Analyse-VM gesendet. Beispiel: Übermittelt ein Benutzer die URL "http://the.earth.li/~sgtatham/putty/latest/x86/putty.exe", wird die Datei "putty.exe" auf die Advanced Threat Defense Appliance heruntergeladen und anschließend an die Analyse-VM gesendet.

Wenn Sie mithilfe der Advanced Threat Defense-Web-Anwendung eine URL zur Analyse senden, wählen Sie ein Analyseprofil aus. Dieses Analyseprofil setzt das mit Ihrem Benutzerkonto verknüpfte Standard-Analyseprofil außer Kraft.

Manuelles Hochladen mithilfe der URL-Option

Vorgehensweise

1 Wählen Sie **Analyse** | **Manual Upload (Manuelles Hochladen)** aus.

2 Auf der Seite **Manual Upload** legen Sie die Details gemäß Ihren Anforderungen fest.

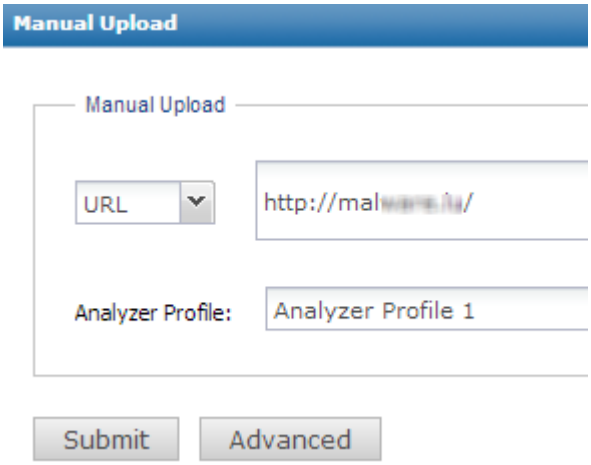


Abbildung 7-8 Senden einer URL zur Malware-Analyse

Tabelle 7-3 Optionsbeschreibungen

Option	Beschreibung
URL Upload method (URL-Upload-Methode)	Wählen Sie in der Dropdownliste eine Upload-Methode aus: • **URL** – Die URL wird direkt auf der Analyse-VM analysiert. • **URL Download** (URL-Download) – Die von der URL genannte Datei wird in die Advanced Threat Defense Appliance und anschließend zur Analyse auf die Analyse-VM heruntergeladen. Nur HTTP, HTTPS und FTP werden unterstützt. Geben Sie daher die Protokoll-ID in der URL an. Geben Sie möglichst die gesamte URL ein. Wenn Advanced Threat Defense die URL dynamisch analysiert, könnte der Browser fehlende Elemente hinzufügen. Wenn Sie zum Beispiel `http://google.com` eingeben, könnte der Browser der Analyse-VM Ihre Eingabe in `http://www.google.com` ändern.
Analyseprofil	Wählen Sie das für die Probe erforderliche Analyseprofil. Es werden nur Analyseprofile aufgeführt, die über die Internetzugriffsoptionen "Sandbox" (Sandkasten) und "Malware" verfügen.

Tabelle 7-3 Optionsbeschreibungen *(Fortsetzung)*

Option	Beschreibung
Erweitert	Klicken Sie auf diese Option, um den interaktiven Benutzermodus zur Analyse der URL anzugeben. Die Option **Erweitert** steht nur zur Verfügung, wenn Sie die Datei manuell mittels McAfee Advanced Threat Defense-Web-Anwendung senden. Manche Malware erfordert nach der Ausführung eine Benutzereingabe. Dadurch wird in der Regel überprüft, ob die Malware in einem Sandkasten analysiert wird. Falls keine Benutzereingabe erfolgt, wählt die Malware möglicherweise einen anderen Ausführungspfad oder hält die Ausführung sogar an. Bei Auswahl dieser Option können Sie auf die tatsächliche Analyse-VM zugreifen, auf der die Malware ausgeführt wird, und so die Benutzereingabe durchführen. Dieser Vorgang ähnelt dem Ausführen von Dateien im interaktiven Benutzermodus. Siehe Hochladen von URLs zur Analyse im interaktiven Benutzermodus auf Seite 281.
Senden	Klicken Sie zum Hochladen der URL zur Analyse in McAfee Advanced Threat Defense auf diese Schaltfläche. Nachdem die URL erfolgreich hochgeladen wurde, wird ein Meldungsfeld angezeigt. • Dateiname – die von Ihnen gesendete URL • Dateigröße – die Größe der Probe • MD5 – der MD5-Hashwert, wie durch Advanced Threat Defense berechnet • MIME-Typ

3 Klicken Sie auf **Senden**.

Konfigurieren der Seite "Analysis Status" (Analysestatus)

Vorgehensweise

1 Wählen Sie **Analyse** | **Analysis Status (Analysestatus)** aus.

Auf der Seite **Analysis Status** wird der Status der eingesendeten Dateien angezeigt.


Analysis Status
Analysis Results
Manual Upload
Analysis Status
Last 24 hours
Refresh every 1 minute
Samples
Case Sensitive
Search By
Search
mitted Time
Status
File Name
User
VM Profile
Analyzer Profile
MD5
4-10-24 11:08:33 MDT Completed AdbeRdrUpd11009_incr.msp nsp Below minimu...
4-10-24 11:08:33 MDT Completed 2dc1c6ab937c5221c3ff0c719b5c5e5d nsp Below minimu...
4-10-24 11:07:10 MDT Completed surefire-booter-2.16.jar nsp File type not s... F75BB0F2D75CDEF
4-10-24 11:07:10 MDT Analyzing maven-plugin-annotations-3.2.jar nsp winXPsp3 Analyzer Profile 1 BEAD7FF75948592
4-10-24 11:07:10 MDT Completed surefire-booter-2.16.jar nsp File type not s... F75BB0F2D75CDEF
4-10-24 11:07:10 MDT Analyzing bead7ff759485924df2257ea048d6385 nsp winXPsp3 Analyzer Profile 1 BEAD7FF75948592
4-10-24 11:07:08 MDT Completed am_engine_patch1_e54b94a9ea73dd... nsp winXPsp3 Analyzer Profile 1 374CE8F08FAE319
4-10-24 11:07:07 MDT Completed nsp winXPsp3 Analyzer Profile 1 374CE8F08FAE319
4-10-24 11:06:57 MDT Analyzing maven-surefire-plugin-2.16.jar nsp winXPsp3 Analyzer Profile 1 364CDA98D192CD

Abbildung 7-9 Status der zur Analyse eingesendeten Dateien

Wenn Sie keine Administratorberechtigungen haben, werden nur die von Ihnen eingesendeten Dateien angezeigt. Ein Benutzer mit Administratorberechtigungen kann von allen Benutzern eingesendete Dateien sehen.

2 Wählen Sie aus der Dropdown-Liste die Kriterien zum Anzeigen und Aktualisieren des Status der analysierten Dateien aus.

- Legen Sie die Kriterien zum Anzeigen von Datensätzen auf der Seite **Analysis Status** (Analysestatus) fest.

  Das Standardintervall für die Aktualisierung beträgt 1 Minute.

- Legen Sie das Zeitintervall für die Aktualisierung der Seite **Analysis Status** (Analysestatus) fest.

  Standardmäßig werden die Ergebnisse der letzten 24 Stunden angezeigt. Sie können diese Kriterien basierend auf Zeit oder Anzahl festlegen. Beispielsweise können Sie den Status von Dateien anzeigen, die in den letzten 5 Minuten eingesendet wurden, oder den der letzten 100 Proben.



Um die Seite "Analysis Status" (Analysestatus) jetzt zu aktualisieren, klicken Sie auf  .

3 Filtern Sie die angezeigten Datensätze, um diejenigen zu finden, nach denen Sie suchen.

Tabelle 7-4 Filteroptionen

Option	Beschreibung
Search (Suche)	Geben Sie den Parameter an, den Sie zum Filtern der Datensätze verwenden möchten. Klicken Sie auf **Search** (Suche), und wählen Sie einen oder mehrere der folgenden Parameter: • Legen Sie die Kriterien zum Anzeigen von Datensätzen auf der Seite **Analysis Status** (Analysestatus) fest. • **File Name** (Dateiname): Wählen Sie diesen Parameter, wenn Sie nach dem Beginn des Dateinamens filtern möchten. Wenn Sie beispielsweise diese Option wählen und *cal* als Suchbegriff eingeben, wird der Status der Dateien aufgeführt, deren Name mit *cal* beginnt. • **MD5**: Wählen Sie diesen Parameter, wenn Sie nach dem Beginn des MD5-Hashwerts filtern möchten. • **VM Profile** (VM-Profil): Wählen Sie diesen Parameter, wenn Sie nach den verfügbaren VM-Profilen filtern möchten. • **File Type** (Dateityp): Das zur Analyse eingesendete Dateiformat. • **Analyzer Profile** (Analyseprofil): Das für die Analyse verwendete Analyseprofil. Wenn die Datei nur statisch analysiert wurde, wird dies angezeigt. • **User** (Benutzer): Der Anmeldename des Benutzers, der die Datei zur Analyse eingesendet hat. • **Source IP** (Quell-IP): Die IP-Adresse des Hosts, der die analysierte Datei gesendet hat. Dies ist nur für Dateien relevant, die automatisch von anderen McAfee-Produkten wie Network Security Platform eingesendet werden. • **Destination IP** (Ziel-IP): Die IP-Adresse des Zielhosts. Ähnlich wie die Quell-IP ist dies nicht relevant für manuell eingesendete Dateien. • **Job ID** (Auftrags-ID): Dies ist eine allen Dateien zugewiesene eindeutige Nummer. • **Task ID** (Task-ID): Dies ist eine allen Dateien zugewiesene eindeutige Nummer. Die **Task ID** (Task-ID) und die **Job ID** (Auftrags-ID) unterscheiden sich für komprimierte Dateien und sind für nicht komprimierte Dateien identisch. • **URL**: Liste der zur Analyse eingesendeten URLs. Geben Sie den Suchbegriff im Textfeld daneben ein.
Case Sensitive (Groß-/Kleinschreibung beachten)	Wählen Sie diese Option, wenn bei der Suche die Groß-/Kleinschreibung beachtet werden soll.

Nehmen wir an, Sie haben **File Name** (Dateiname) und **Status** als Kriterien ausgewählt sowie den Begriff **Com** mit der Option *Case Sensitive* (Groß-/Kleinschreibung beachten) festgelegt. Alle Datensätze mit dem Status "Completed" (Abgeschlossen) und Dateinamen, die mit *Com* beginnen, werden aufgeführt.

Tabelle 7-5 Spaltendefinitionen

Spalte	Beschreibung
Submitted Time (Übermittlungszeit)	Ein Zeitstempel, der angibt, wann die Datei zur Analyse übermittelt wurde.
Status	Der aktuelle Status der Analyse. • **Waiting** (Warten) – Typischerweise weist dieser Status darauf hin, dass McAfee Advanced Threat Defense auf die dynamische Analyse der Datei durch die Analyse-VM wartet. • **Analyzing** (Analysieren) – Gibt an, dass die Analyse noch läuft. • **Completed** (Abgeschlossen) – Gibt an, dass die Analyse der Datei abgeschlossen ist. Doppelklicken Sie auf den Datensatz, um den vollständigen Bericht anzuzeigen.
File Name (Dateiname)	Der Name der Datei, die Sie zur Analyse eingesendet haben.
VM Profile (VM-Profil)	Das für die dynamische Analyse verwendete VM-Profil. Wenn die Datei nur statisch analysiert wurde, wird dies angezeigt.
MD5	Der MD5-Hash-Wert der Datei, wie durch McAfee Advanced Threat Defense berechnet.
Analyzer Profile (Analyseprofil)	Das für die Analyse verwendete Analyseprofil. Wenn die Datei nur statisch analysiert wurde, wird dies angezeigt.
User (Benutzer)	Der Anmeldename des Benutzers, der die Datei zur Analyse eingesendet hat.
Source IP (Quell-IP)	Die IP-Adresse des Hosts, der die analysierte Datei gesendet hat. Dies ist nur für Dateien relevant, die automatisch von anderen McAfee-Produkten wie Network Security Platform eingesendet werden.
Destination IP (Ziel-IP)	Die IP-Adresse des Zielhosts. Ähnlich wie die Quell-IP ist dies nicht relevant für manuell eingesendete Dateien.

4 Blenden Sie die Spalten aus, die Sie nicht benötigen.

a Bewegen Sie den Mauszeiger über die rechte Ecke einer Spaltenüberschrift, und klicken Sie auf den Dropdown-Pfeil.

b Wählen Sie **Columns** (Spalten).

c Wählen Sie nur die erforderlichen Spaltennamen aus der Liste.

Sie können auf eine Spaltenüberschrift klicken und sie an die gewünschte Position ziehen.

5 Zum Sortieren der Datensätze basierend auf einem bestimmten Spaltennamen klicken Sie auf die Spaltenüberschrift.

Sie können die Datensätze in auf- oder absteigender Reihenfolge sortieren. Alternativ können Sie den Mauszeiger über die rechte Ecke einer Spaltenüberschrift bewegen und auf den Dropdown-Pfeil klicken. Wählen Sie dann **Sort Ascending** (Aufsteigend sortieren) oder **Sort Descending** (Absteigend sortieren). In der Standardeinstellung werden die Datensätze in absteigender Reihenfolge der Spalte **Submitted Time** (Übermittlungszeit) sortiert.

6 Klicken Sie auf , um die Einstellungen der Seite "Analysis Results" (Analyseergebnisse) zu speichern.

Anzeigen der Analyseergebnisse

Nachdem Sie eine Datei zur Analyse eingesendet haben, können Sie die Ergebnisse auf der Seite **Analysis Results** (Analyseergebnisse) anzeigen.

Ältere Berichte werden gelöscht, sobald der Datenspeicher von McAfee Advanced Threat Defense zu 75 % voll ist. Sie können den aktuell verfügbaren Datenspeicherplatz auf dem Monitor **System Health** (Systemzustand) des **Dashboards** anzeigen. Wenn Sie die Optionen unter **FTP Result Output** (FTP-Ergebnisausgabe) auf der Seite **Benutzerverwaltung** konfigurieren, speichert McAfee Advanced Threat Defense die Ergebnisse lokal und sendet sie zur langfristigen Nutzung an den konfigurierten FTP-Server.

Vorgehensweise

1 Wählen Sie **Analyse** | **Analysis Results (Analyseergebnisse)** aus.

Auf der Seite **Analysis Results** wird der Status der abgeschlossenen Dateien angezeigt.

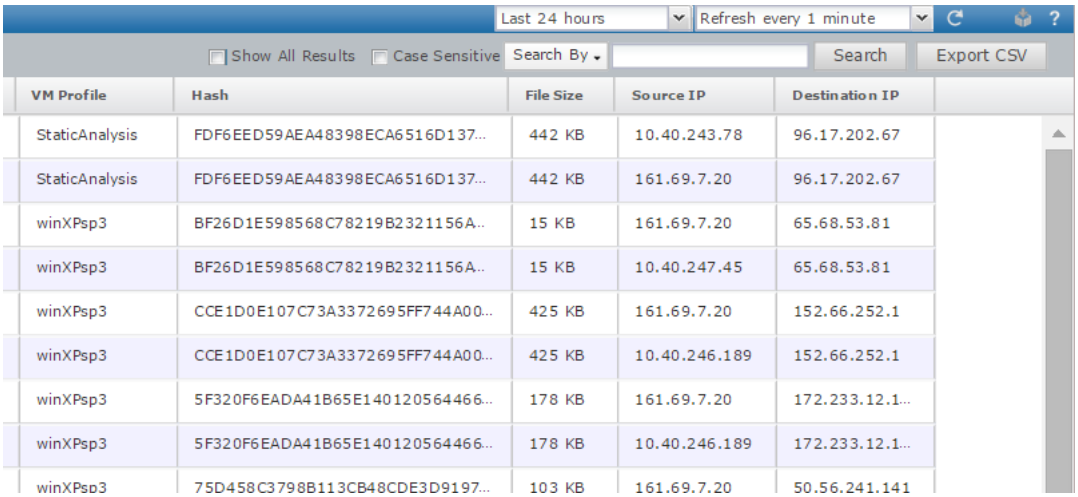


Abbildung 7-10 Status der zur Analyse eingesendeten Dateien

Wenn Sie keine Administratorberechtigungen haben, werden nur die von Ihnen eingesendeten Dateien angezeigt. Ein Benutzer mit Administratorberechtigungen kann von allen Benutzern eingesendete Dateien sehen.

Klicken Sie auf **Export CSV** (CSV exportieren), um den Status der abgeschlossenen Dateien im CSV-Format lokal zu exportieren.

2 Legen Sie die Kriterien zum Anzeigen und Aktualisieren der Datensätze auf der Seite **Analysis Results** fest.

a Legen Sie die Kriterien zur Datensatzanzeige auf der Seite **Analysis Results** fest.

Standardmäßig werden die Ergebnisse der in den letzten 24 Stunden abgeschlossenen Dateien angezeigt.

Sie können diese Kriterien basierend auf Zeit oder Anzahl festlegen. Beispielsweise können Sie Dateien anzeigen, deren Analyse in den letzten 5 Minuten abgeschlossen wurde, oder die letzten 100 abgeschlossenen Dateien.

b Legen Sie das Zeitintervall für die automatische Aktualisierung der Seite **Analysis Results** fest.

Das Standardintervall für die Aktualisierung beträgt 1 Minute.

c Um die Seite **Analysis Results** jetzt zu aktualisieren, klicken Sie auf .

Tabelle 7-6 Spaltendefinitionen

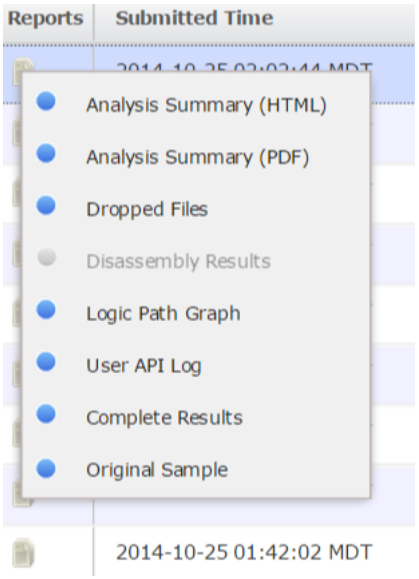
Spalte	Beschreibung
Reports (Berichte)	Klicken Sie auf , damit die für die Probe verfügbaren Berichtarten angezeigt werden.  Klicken Sie auf einen beliebigen aktivierten Bericht, um die zugehörigen Details anzuzeigen. Ein spezieller Bericht wird nur aktiviert, wenn er für die analysierte Datei relevant und außerdem im zugehörigen Analyseprofil ausgewählt ist. • **Analysis Summary (HTML)** (Analyseübersicht (HTML)) – Dabei handelt es sich um einen umfassenden Bericht, der für alle Dateitypen verfügbar ist. Dieser Bericht wird auch angezeigt, wenn Sie auf einen Datensatz doppelklicken. • **Analysis Summary (PDF)** (Analyseübersicht (PDF)) – Wählen Sie diese Option, um den Bericht im PDF-Format anzuzeigen. • **Dropped Files** (Betroffene Dateien) – Wählen Sie diesen Bericht, um die Dateien anzuzeigen, die während der dynamischen Analyse von der analysierten Probe erstellt wurden. • **Disassembly Results** (Disassembly-Ergebnisse) – Wählen Sie diese Option, um den von der Datei per Reverse Engineering erstellten Assembly-Sprachcode anzuzeigen. Dieser Bericht eignet sich nur für Probedateien wie .exe und .dll. • **Logic Path Graph** (Logisches Pfaddiagramm) – Wählen Sie diese Option, um eine grafische Darstellung der während der dynamischen Analyse ausgeführten Subroutinen anzuzeigen. • **Dynamic Execution Logs** (Dynamische Ausführungsprotokolle) – Wählen Sie diese Option, um die während der dynamischen Analyse direkt

Tabelle 7-6 Spaltendefinitionen *(Fortsetzung)*

Spalte	Beschreibung
	über die Probe ausgeführten Windows-DLL-API-Aufrufe auf Benutzerebene anzuzeigen. • **Complete Results** (Vollständige Ergebnisse) – Klicken Sie hier, um eine ZIP-Datei mit allen Berichtsarten auf Ihren lokalen Computer herunterzuladen. • **Original Sample** (Originalprobe) – Klicken Sie hier, um die gesendete Originalprobe herunterzuladen.
Submitted Time (Übermittlungszeit)	Ein Zeitstempel, der angibt, wann die Datei zur Analyse übermittelt wurde.
Schweregrad	Der Schweregrad der gesendeten Datei.
File Name (Dateiname)	Der Name der Datei, die Sie zur Analyse eingesendet haben.
Benutzer	Der Anmeldename des Benutzers, der die Datei zur Analyse eingesendet hat.
Analyseprofil	Das für die Analyse verwendete Analyseprofil.
VM-Profil	Das für die dynamische Analyse verwendete VM-Profil. Wenn nur die statische Analyse ausgeführt wurde, wird dies angezeigt.
Hash	Der MD5-Hash-Wert der Datei, wie durch McAfee Advanced Threat Defense berechnet.
Dateigröße	Die Größe der analysierten Datei in KB.
Source IP (Quell-IP)	Die IP-Adresse des Hosts, der die analysierte Datei gesendet hat. Dies ist nur für Dateien relevant, die automatisch von anderen McAfee-Produkten wie Network Security Platform eingesendet werden.
Destination IP (Ziel-IP)	Die IP-Adresse des Zielhosts. Ähnlich wie die Quell-IP ist dies nicht relevant für manuell eingesendete Dateien.

3 Blenden Sie die Spalten aus, die Sie nicht benötigen.

a Bewegen Sie den Mauszeiger über die rechte Ecke einer Spaltenüberschrift, und klicken Sie auf den Dropdown-Pfeil.

b Wählen Sie **Columns** (Spalten).

c Wählen Sie nur die erforderlichen Spaltennamen aus der Liste.

Sie können auf eine Spaltenüberschrift klicken und sie an die gewünschte Position ziehen.

4 Zum Sortieren der Datensätze basierend auf einem bestimmten Spaltennamen klicken Sie auf die Spaltenüberschrift.

Sie können die Datensätze in auf- oder absteigender Reihenfolge sortieren. Alternativ können Sie den Mauszeiger über die rechte Ecke einer Spaltenüberschrift bewegen und auf den Dropdown-Pfeil klicken. Wählen Sie dann **Sort Ascending** (Aufsteigend sortieren) oder **Sort Descending** (Absteigend sortieren).

Standardmäßig werden die Dateien mit hohem Schweregrad oben in der Liste angezeigt.

5 Klicken Sie auf  , um die Einstellungen der Seite "Analysis Results" (Analyseergebnisse) zu speichern.

Anzeigen des Berichts "Analysis Summary" (Analyseübersicht)

Im Übersichtsbericht der Analyse werden die zentralen Verhaltensweisen der Probedatei beschrieben. Dieser Bericht ist in den Formaten HTML, Text, PDF, XML, JSON, OpenIOC (Open Indicators of Compromise) und STIX (Structured Threat Information eXpression) erhältlich.

Die HTML, Text- und PDF-Formate dienen hauptsächlich zum Lesen und Prüfen des Analyseberichts. Auf die HTML- und PDF-Formate können Sie über die McAfee Advanced Threat Defense-Web-Anwendung zugreifen. Die HTML- und Textformate sind außerdem in der ZIP-Berichtedatei für die Probe verfügbar, die Sie auf Ihren Client-Computer herunterladen können.

Die XML- und JSON-Formate enthalten Verhaltenstags bekannter Malware für Programmierungsskripte, sodass Schlüsselinformationen extrahiert werden können. Network Security Platform und McAfee Web Gateway zeigen die Berichtsdetails mittels JSON-Formaten in ihren Benutzeroberflächen an.

Ab einem Schweregrad der Probe von 3 ist der Übersichtsbericht der Analyse in den Formaten OpenIOC (.ioc) und STIX (.stix.xml) verfügbar. Die OpenIOC- und STIX-Formate sind allgemein anerkannte Formate für die Freigabe von Bedrohungsinformationen. Diese Formate machen es möglich, Übersichtsberichte der Analyse für andere Sicherheitsanwendungen effizient freizugeben, um Malware besser verstehen, erkennen und eindämmen zu können. Sie können die OpenIOC- und STIX-Berichte beispielsweise manuell an eine Anwendung senden, die Hosts nach Indikatoren im Bericht abfragen kann. Auf diese Weise können Sie die infizierten Hosts erkennen und dann die erforderlichen Maßnahmen zur Eindämmung und Entfernung der Malware ergreifen.

Generische Informationen zu OpenIOC erhalten Sie unter http://www.openioc.org/. Informationen zu STIX erhalten Sie unter https://stix.mitre.org/. Der Übersichtsbericht der Analyse in den OpenIOC- und STIX-Formaten ist in der ZIP-Datei "Complete Results" (Vollständige Ergebnisse) für die Probe verfügbar.

Vorgehensweise

1. Führen Sie folgende Schritte aus, um den Übersichtsbericht der Analyse in der McAfee Advanced Threat Defense-Web-Anwendung anzuzeigen:
   a. Wählen Sie **Analyse** | **Analysis Results (Analyseergebnisse)** aus.
   b. Um den Bericht im HTML-Format anzuzeigen, klicken Sie auf , und wählen Sie **Analysis Summary (HTML)** (Analyseübersicht (HTML)).
      Alternativ können Sie auf den gewünschten Datensatz doppelklicken.
   c. Um den Bericht im PDF-Format anzuzeigen, klicken Sie auf , und wählen Sie **Analysis Summary (PDF)** (Analyseübersicht (PDF)).
2. Führen Sie folgende Schritte aus, um den Übersichtsbericht der Analyse über die ZIP-Berichtedatei zu öffnen:
   a. Wählen Sie **Analyse** | **Analysis Results (Analyseergebnisse)** aus.
   b. Klicken sie auf , und wählen Sie **Complete Results** (Vollständige Ergebnisse) aus.
   c. Speichern Sie die komprimierten Berichte auf Ihrem lokalen Computer.
      Die ZIP-Datei wird nach der Probedatei benannt.
   d. Extrahieren Sie die Inhalte der ZIP-Datei.
      Der AnalysisLog-Ordner enthält den Analysebericht im HTML-, Text-, XML- und JSON-Format. Ab einem Malware-Schweregrad von 3 sind auch OpenIOC- und STIX-Formate enthalten. Sie können diese Dateien anhand des Namens der Malware-Datei identifizieren. Der Name der

Malware-Datei wird hinzugefügt zu _summary.html, _summary.json, _summary.txt, _summary.xml, _summary.ioc und _summary.stix.xml.

Im Folgenden sind die verschiedenen Abschnitte der HTML-Version des Übersichtsberichts der Analyse dargestellt.

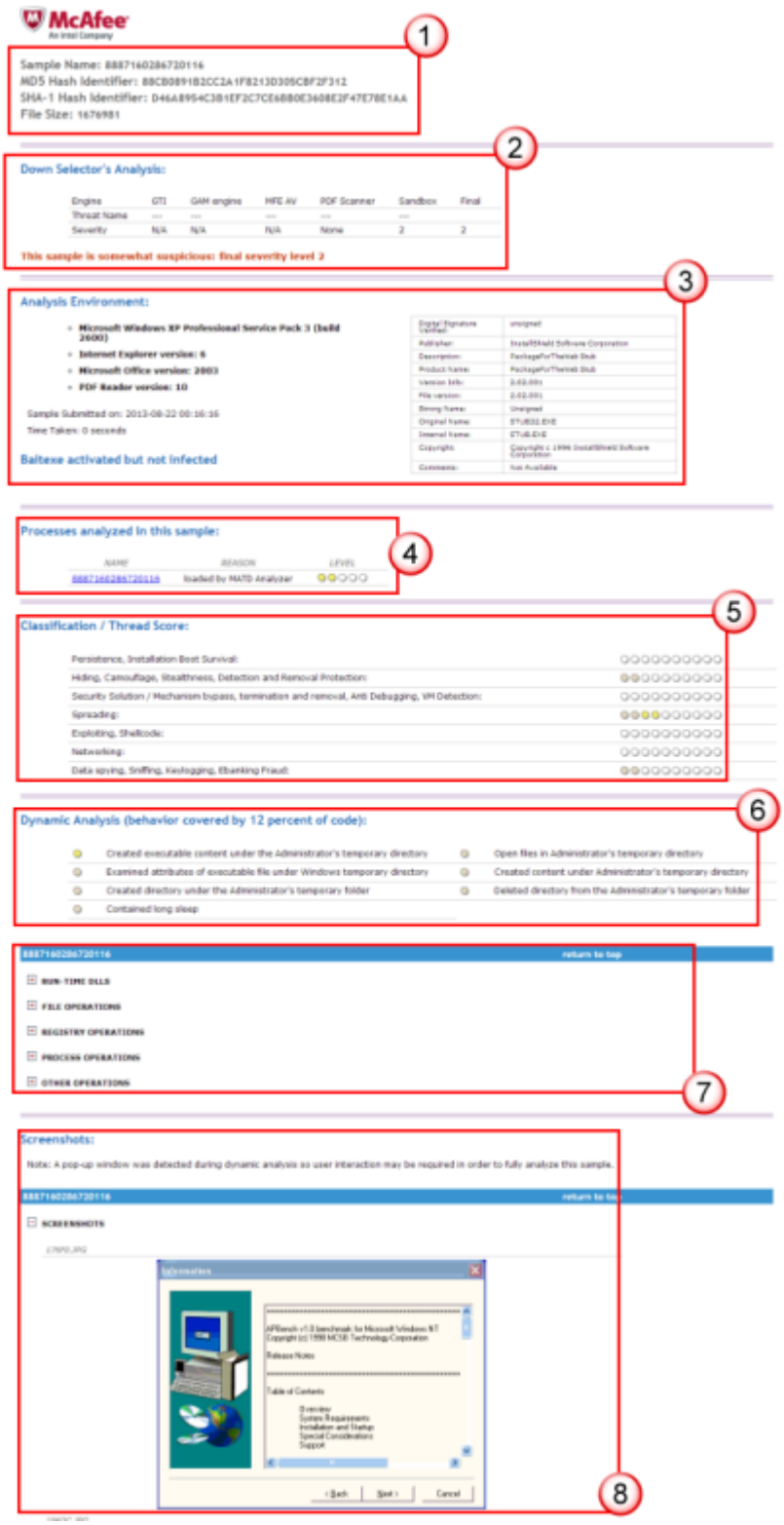

McAfee
1
Sample Name: 8887160286720116
MD5 Hash Identifier: 88CB0891B2CC2A1F8213D305CBF2F312
SHA-1 Hash Identifier: D46A8954C3B1EF2C7CE6BB0E3608E2F47E70E1AA
File Size: 1679981
2
Down Selector's Analysis:
Engine GTI GAM engine HFE AV PDF Scanner Sandbox Final
Threat Name --- --- --- --- --- ---
Severity N/A N/A N/A None 2 2
This sample is somewhat suspicious: final severity level 2
3
Analysis Environment:
Microsoft Windows XP Professional Service Pack 3 (build 2600)
Internet Explorer version: 6
Microsoft Office version: 2003
PDF Reader version: 10
Sample Submitted on: 2013-08-22 00:16:16
Time Taken: 0 seconds
Baltexe activated but not infected
4
Processes analyzed in this sample:
NAME REASON LEVEL
8887160286720116 loaded by MATD Analyzer
5
Classification / Thread Score:
Persistence, Installation Boot Survival:
Hiding, Camouflage, Stealthness, Detection and Removal Protection:
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection:
Spreading:
Exploiting, Shellcode:
Networking:
Data spying, Sniffing, Keylogging, Ebanking Fraud:
6
Dynamic Analysis (behavior covered by 12 percent of code):
Created executable content under the Administrator's temporary directory
Examined attributes of executable file under Windows temporary directory
Created directory under the Administrator's temporary folder
Contained long sleep
Open files in Administrator's temporary directory
Created content under Administrator's temporary directory
Deleted directory from the Administrator's temporary folder
8887160286720116 return to top
RUN-TIME DLLS
FILE OPERATIONS
REGISTRY OPERATIONS
PROCESS OPERATIONS
OTHER OPERATIONS
7
Screenshots:
Note: A pop-up window was detected during dynamic analysis so user interaction may be required in order to fully analyze this sample.
8887160286720116 return to to
SCREENSHOTS
8

Abbildung 7-11 Übersichtsbericht der Analyse

Tabelle 7-7 Abschnitte des Übersichtsberichts der Analyse

Element	Beschreibung
1	Dieser Abschnitt enthält Details zur Probedatei. Dazu gehören Name, Hash-Werte und die Dateigröße in Byte.
2	Abschnitt "Analysis results" (Analyseergebnisse). auf Seite 301. Dieser Abschnitt enthält die Ergebnisse der auf die Datei angewendeten Methoden. Außerdem wird der Schweregrad für die Datei angegeben.
3	Abschnitt "Analysis Environment" auf Seite 302. Dieser Abschnitt enthält Details zu Analyse-VM, Eigenschaften der Datei usw.
4	"Processes analyzed in this sample" (In dieser Probe analysierte Prozesse). In diesem Abschnitt werden alle Dateien aufgeführt, die bei der dynamischen Analyse der Probedatei ausgeführt wurden. Des Weiteren wird der Grund für das Ausführen jeder Datei angegeben, zusammen mit deren Schweregrad. In der Spalte "Reason" (Grund) wird aufgeführt, welche anderen Dateien oder Prozesse diese Datei erstellt oder geöffnet haben. Enthält die Probe nur eine Datei, wird als Grund *loaded by MATD Analyzer* (geladen von MATD Analyzer) angezeigt. Wenn es sich bei der Probedatei um eine ZIP-Datei mit mehreren Dateien handelt oder wenn eine Datei andere Dateien öffnet, lautet der Grund für die erste Datei *created by <file name> & loaded by MATD Analyzer* (erstellt von <Dateiname> und geladen von MATD Analyzer). Für die folgenden Dateien werden in der Spalte "Reason" alle Dateien/Prozesse angegeben, die sie erstellt und geöffnet haben. In der Spalte "Ebene" wird der Schweregrad jeder Datei basierend auf der dynamischen Analyse angegeben. • ○○○○○ – gibt einen Schweregradfaktor von 0 und die Bedrohungsstufe "Information" an. Dies ist der Schweregrad für als sicher klassifizierte Dateien. • ●○○○○ – gibt einen Schweregradfaktor von 1 und eine sehr niedrige Bedrohungsstufe an. • ●●○○○ – gibt einen Schweregradfaktor von 2 und eine niedrige Bedrohungsstufe an. • ●●●○○ – gibt einen Schweregradfaktor von 3 und eine mittlere Bedrohungsstufe an. • ●●●●○ – gibt einen Schweregradfaktor von 4 und eine hohe Bedrohungsstufe an. • ●●●●● – gibt einen Schweregradfaktor von 5 und eine sehr hohe Bedrohungsstufe an. Klicken Sie auf einen Dateinamen, um zu dem Abschnitt des Berichts zu navigieren, der Details zum Verhalten der Datei enthält. Beim Klicken auf einen Dateinamen springen Sie also zu Abschnitt 7 der obigen Abbildung.
5	Abschnitt "Classification/Threat Score" auf Seite 303 Dieser Abschnitt enthält die individuellen Faktoren der unterschiedlichen Merkmale einer typischen Malware.

Tabelle 7-7 Abschnitte des Übersichtsberichts der Analyse *(Fortsetzung)*

Element	Beschreibung
6	Abschnitt "Dynamic Analysis" (Dynamische Analyse). Dieser Abschnitt gibt den Prozentsatz des ausgeführten Dateicodes an. Beispielsweise folgte die Datei vielleicht während der Ausführung einem alternativen Pfad, weswegen ein Teil des Codes überhaupt nicht ausgeführt wurde. In diesem Abschnitt finden Sie auch eine kurze Übersicht über das Verhalten, zusammen mit den entsprechenden Schweregraden. gibt ein Verhalten mit sehr niedrigem Schweregrad an. gibt ein Verhalten mit niedrigem Schweregrad an. gibt ein Verhalten mit mittlerem Schweregrad an. gibt ein Verhalten mit hohem Schweregrad an. gibt ein Verhalten mit sehr hohem Schweregrad an.
7	Abschnitt "Operations details" (Vorgangsdetails). Dieser Abschnitt enthält detaillierte Informationen zu allen Vorgängen, die die Probedatei während der dynamischen Analyse ausgeführt hat. Diese Vorgänge sind in sinnvolle Gruppen unterteilt. Erweitern Sie die Gruppen, um die einzelnen Vorgänge anzuzeigen. Erweitern Sie zum Beispiel **Files Operations** (Dateivorgänge), um die erstellten, gelöschten, geänderten und gelesenen Dateien sowie erstellte, geöffnete oder entfernte Verzeichnisse usw. anzuzeigen.
8	GTI-URL-Reputation. Gibt dieMcAfee GTI-Reputation und den Schweregrad für die URL an.
9	"Network activity" (Netzwerkaktivität). Dieser Abschnitt enthält Details zu jedem Netzwerkvorgang während der dynamischen Analyse der Probe.
10	Abschnitt "Screenshots". Dieser Abschnitt enthält alle während der dynamischen Analyse angezeigten Popupfenster. Mithilfe dieser Screenshots können Sie festlegen, ob während der dynamischen Analyse ein Eingreifen seitens des Benutzers erforderlich ist, um das tatsächliche Verhalten der Datei zu bestimmen. Falls ein Benutzereingreifen erforderlich ist, können Sie die Datei im interaktiven Benutzermodus manuell versenden.

Abschnitt "Analysis results" (Analyseergebnisse).

Dies ist ein Abschnitt im Übersichtsbericht der Analyse. Darin können Sie anzeigen, durch welche Methoden berichtet wurde, dass die Beispieldatei Malware enthält.

Tabelle 7-8 Analyseauswahl

Beschriftung	Beschreibung
Engine (Modul)	Dies sind die verschiedenen Methoden, die McAfee Advanced Threat Defense zur Dateianalyse verwendet. • GTI File Reputation: bezieht sich auf das McAfee GTI-Modul, das sich in der Cloud befindet • Gateway Anti-Malware: steht für McAfee Gateway Anti-Malware Engine • Anti-Malware: Verweist auf McAfee Anti-Malware Engine • Sandbox: zeigt an, dass die Datei auf einer Analyse-VM ausgeführt wurde; Details zu dieser VM finden Sie im "Analysis Environment"-Abschnitt (Analyseumgebung) des Berichts
Threat Name (Bedrohungsname)	Dies zeigt den Namen bekannter Malware inMcAfee GTI, McAfee Gateway Anti-Malware Engine und McAfee Anti-Malware Engine an.
Severity (Schweregrad)	Diese Beschriftung zeigt den von verschiedenen Methoden angegebenen Schweregradfaktor. Der höchste Faktor einer bestimmten Methode wird verwendet, um den endgültigen Schweregrad für die Probe festzulegen.

Abschnitt "Analysis Environment"

Dies ist ein Abschnitt im Übersichtsbericht der Analyse. In diesem Abschnitt finden Sie die folgenden Details:

- Details der entsprechenden Analyse-VM wie Betriebssystem, Browser und Version sowie die Anwendungen, die auf der VM installiert sind, und ihre Versionen

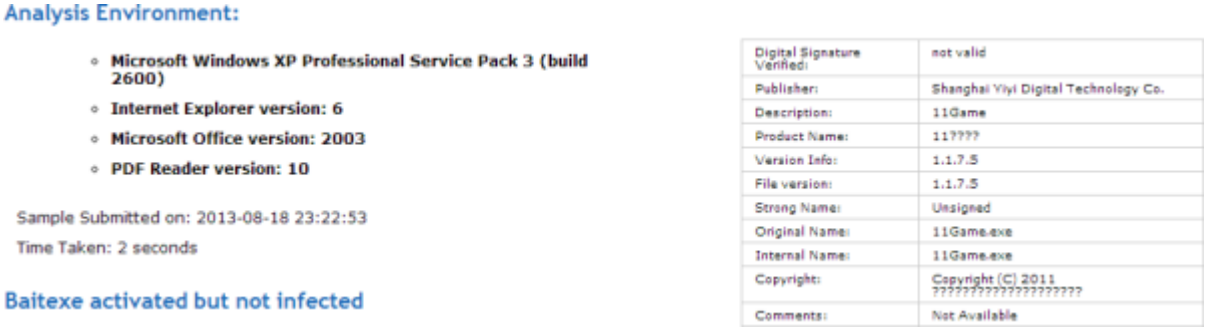

Analysis Environment:
Microsoft Windows XP Professional Service Pack 3 (build 2600)
Internet Explorer version: 6
Microsoft Office version: 2003
PDF Reader version: 10
Sample Submitted on: 2013-08-18 23:22:53
Time Taken: 2 seconds
Baitexe activated but not infected
Digital Signature Verified: not valid
Publisher: Shanghai Yiyi Digital Technology Co.
Description: 11Game
Product Name: 11????
Version Info: 1.1.7.5
File version: 1.1.7.5
Strong Name: Unsigned
Original Name: 11Game.exe
Internal Name: 11Game.exe
Copyright: Copyright (C) 2011 ??????????????????
Comments: Not Available

Abbildung 7-12 Abschnitt "Analysis Environment"

- Die Zeit, wenn die Probe gesendet wurde, wie von der Uhr der McAfee Advanced Threat Defense-Appliance angegeben
- Die benötigte Zeit für die Dateianalyse und die Berichterstellung
- Auf der rechten Seite gibt eine Tabelle die Dateieigenschaften an. Diese enthält unter anderem folgende Informationen:
  - Digitale Signatur für die Datei vorhanden oder nicht
  - Name des Herausgebers, falls vorhanden

  - Versionsinformationen
  - Originalname der Datei, sodass Sie in anderen Quellen, etwa dem Internet, danach suchen können.

- *Baitexe-Vorgang:* infiziert oder nicht. Am Ende jeder Analyse erstellt McAfee Advanced Threat Defense einen zusätzlichen Köder-Vorgang namens Baitexe. Das Baitexe-Programm ruft nur zwei APIs ("beep" und "sleep") kontinuierlich auf. Wenn dieser Baitexe-Vorgang von der zuvor ausgeführten Probe infiziert wurde, ändert sich das Verhalten von Baitexe. In diesem Fall wird die Nachricht *Baitexe activated and infected* (Baitexe ist aktiviert und infiziert) angezeigt. Wenn der Baitexe-Vorgang nicht infiziert ist, wird die Meldung *Baitexe activated but not infected* (Baitexe ist aktiviert, aber nicht infiziert) angezeigt.

Abschnitt "Classification/Threat Score"

Dies ist ein Abschnitt im Übersichtsbericht der Analyse, in dem der Schweregrad für verschiedene Merkmale einer typischen Malware angegeben sind.

Tabelle 7-9 Abschnitt "Classification/Threat Score"

Beschriftung	Beschreibung
Persistence, Installation Boot Survival	Einige Malware hat die Fähigkeit, auf dem infizierten Host zu bleiben. Dies wird als "Persistence" (Persistenz) bezeichnet. "Installation Boot Survival" bezieht sich auf die Fähigkeit der Malware, selbst nach einem Neustart bestehen zu bleiben.
Hiding, Camouflage, Stealthness, Detection und Removal Protection	Dies ist die Fähigkeit einer Malware, Erkennung und Entfernung zu umgehen.
Security Solution/Mechanism Bypass, Termination and Removal, Anti Debugging, VM Detection	Dies ist die Fähigkeit einer Malware, Erkennungsmethoden und -module zu umgehen oder in die Irre zu führen. Einige Malware verfügt über einen Anti-Disassembly-Code, der zu Verwechslungen oder Verzögerungen bei der Malware-Analyse führen kann. Einige Malware-Programme versuchen festzustellen, ob sie in einer Sandkastenumgebung ausgeführt werden. Wenn ja, wählen sie möglicherweise einen anderen Ausführungspfad. Dieser Faktor weist auf das Vorhandensein eines solchen Codes in der Malware hin.
Spreading	Dies ist die Fähigkeit einer Malware, sich im Netzwerk zu verbreiten.
Exploiting, Shellcode	Dies zeigt das Vorhandensein von Shell-Code an, der ein ausgeführtes Programm ausnutzen kann.
Networking	Dies zeigt das netzwerkbezogene Verhalten der Malware während der dynamischen Analyse an. Die Malware könnte beispielsweise DNS-Abfragen ausgelöst oder Sockets erstellt haben. Wenn für dieses Merkmal ein Schweregrad angegeben ist, wird dieser mit den Netzwerkdetails für die Dateien in der Probe abgeglichen.
Data Spying, Sniffing, Keylogging, Ebanking Fraud	Dies zeigt an, ob die Malware zu Datenspionage, Sniffing, Keylogging oder Online-Banking-Betrug fähig ist.

Abschnitt zu Vorgangsdetails

Dieser Abschnitt enthält Details zu jedem Vorgang, der von einer Datei während der dynamischen Analyse ausgeführt wird. Für jede Datei, die als Teil der Probe ausgeführt wurde, gibt es einen separaten Abschnitt.

- Run-time DLLs (Laufzeit-DLLs): Listet alle DLLs und ihre Pfade auf, die von einer Datei während der Laufzeit aufgerufen wurden.
- File operations (Dateivorgänge): Listet Dateivorgangsaktivitäten auf, wie Vorgänge zum Erstellen, Öffnen, Abfragen, Ändern, Kopieren, Verschieben, Löschen sowie Erstellen/Löschen von Verzeichnissen. Dieser Abschnitt enthält auch eine Liste der Dateiattribute und der MD5-Hashwerte für die Dateien.
- Registry operations (Registrierungsvorgänge): Gibt die Details zu Registrierungsvorgangsaktivitäten in Windows an, wie Erstellen/Öffnen, Löschen, Ändern sowie Registrierungsabfragen bei Unter- und Haupteintrittspunkten.
- Process operations (Prozessvorgänge): Gibt Details zu Prozessvorgängen wie die Erstellung neuer Prozesse und Dienste, Beendigung und Codeeinschleusung in andere Prozesse an.
- Networking operations (Netzwerkvorgänge): Gibt Details zu Netzwerkvorgängen wie DNS-Abfragen, TCP-Socketaktivitäten und HTTP-Datei-Downloads an.
- Other operations (Sonstige Vorgänge): Gibt Details von Vorgängen an, die nicht zu den genannten Kategorien gehören. Beispiele dafür sind Mutex-Objekte sowie das Abrufen der Systemmetrik und Konfigurationsdaten der Analyse-VM.

Bericht zu betroffenen Dateien

Sie können eine ZIP-Datei mit allen Dateien herunterladen, die während der dynamischen Analyse von der Probe erstellt oder geöffnet wurden. Sie können diese Dateien mit einer der folgenden Methoden herunterladen:

- Klicken Sie auf der Seite **Analysis Results** (Analyseergebnisse) (**Analyse** | **Analysis Results**)auf  , und wählen Sie **Dropped Files** (Betroffene Dateien) aus. Laden Sie die ZIP-Datei "dropfiles.zip" herunter, die die von der Probe in der Sandkastenumgebung erstellten Dateien enthält. Zum Verwenden dieser Option muss **Dropped Files** im entsprechenden Analyseprofil aktiviert sein.
- Nachdem Sie auf  geklickt haben, wählen Sie **Complete Results** (Vollständige Ergebnisse) aus. Laden Sie die ZIP-Datei "<sample_name>" herunter. Diese ZIP-Datei enthält die gleiche Datei "dropfiles.zip" wie im AnalysisLog-Ordner. "Complete Results" enthält die Datei "<file name>_logicpath.gml", ungeachtet dessen, ob Sie die Option **Dropped Files** im entsprechenden Analyseprofil aktiviert haben.

Disassembly-Ergebnisse

Der Bericht "Disassembly Results" (Disassembly-Ergebnisse) listet die Disassembly-Ausgabe für portable ausführbare Dateien (PE-Dateien) auf. Er wird auf Grundlage der Probedatei generiert, nachdem der Entpackungsvorgang abgeschlossen wurde. Darin sind Informationen zur Malware-Datei, wie etwa der PE-Header, enthalten.

Unter anderem enthält der Bericht "Disassembly Results" die folgenden Informationen:

- Datum und Uhrzeit der Erstellung der Probedatei
- PE-Header und optionale Header-Informationen

- Verschiedene Abschnittsheader-Informationen
- Die Intel-Disassembly-Liste

Sie können den Bericht in der McAfee Advanced Threat Defense-Web-Anwendung anzeigen oder ihn als Datei auf den Client-Computer herunterladen. Die Inhalte des Berichts sind bei beiden Methoden gleich.

- Zum Anzeigen des Berichts "Disassembly Results" in der McAfee Advanced Threat Defense-Web-Anwendung wählen Sie **Analyse** | **Analysis Results** (Analyseergebnisse) aus. Klicken Sie auf der Seite **Analysis Results** (Analyseergebnisse) auf , und wählen Sie **Disassembly Results** (Disassembly-Ergebnisse) aus. Zum Verwenden dieser Option muss **Disassembly Results** im entsprechenden Analyseprofil aktiviert sein.
- Zum Herunterladen einer Berichtsdatei klicken Sie auf der Seite **Analysis Results** auf , und wählen Sie **Complete Results** (Vollständige Ergebnisse) aus. Laden Sie die ZIP-Datei "<sample_name>" herunter. Diese ZIP-Datei enthält im AnalysisLog-Ordner eine Datei mit dem Namen <file name>_detail.asm. Der ZIP-Bericht enthält die ASM-Datei ungeachtet dessen, ob Sie die Option **Disassembly Results** im entsprechenden Analyseprofil aktiviert haben.

Der Bericht "Disassembly Results" umfasst die Assembly-Anweisungen mit allen Aufrufnamen der statischen Standardbibliothek wie printf und DLL-API-Aufrufnamen im Windows-System, die in der Liste eingebettet sind. Wenn globale Variablen wie Zeichenfolgentexte im Code referenziert werden, sind diese ebenfalls aufgeführt.

Tabelle 7-10 Ein Abschnitt eines "Disassembly Results"-Beispielberichts

Spalte 1	Spalte 2	Spalte 3
:00401010	e8 1f2c0000	call 00403c34 ;;call URLDownloadToFileA

Die virtuelle Adresse der Anweisung wird in Spalte 1 angezeigt, die binär codierte Anweisung in Spalte 2 und die Assembly-Anweisung mit Kommentaren in Spalte 3. Im aufgeführten Beispiel führt die Anweisung `call 00403c34` am Speicherort `00401010` einen Funktionsaufruf an den Speicherort `0x403c34` aus. Dabei handelt es sich um einen System-DLL-API-Funktionsaufruf, der als `URLDownloadToFileA()` festgelegt wurde. Der in der Liste angezeigte Kommentar mit `;;` gibt den Bibliotheksfunktionsnamen an.

Bericht "Logic Path Graph" (Logisches Pfaddiagramm)

Dieser Bericht ist eine grafische Darstellung der Querverweise von Funktionsaufrufen, die während der dynamischen Analyse entdeckt wurden. Dadurch können Sie die Subroutinen in der analysierten Datei anzeigen, die während der dynamischen Analyse ausgeführt wurden, sowie diejenigen, die nicht ausgeführt wurden. Diese nicht ausgeführten Funktionen könnten eine potenzielle Zeitbombe darstellen, die unter bestimmten Bedingungen ausgelöst wird.

Der Bericht "Logic Path Graph" ist als GML(Graph Modelling Language)-Datei verfügbar. Dabei handelt es sich um ein reines ASCII-Textformat, das eine grafische Darstellung des logischen Ausführungspfads der Probe im GML-Format enthält. Sie können diese Datei nicht direkt in der McAfee Advanced Threat Defense-Web-Anwendung anzeigen, aber auf Ihren Client-Computer herunterladen. Sie müssen dann ein Grafik-Layout-Programm wie yWorks yEd Graph Editor verwenden, das das GML-Format unterstützt. Mit diesem Editor können Sie die Querverweise aller Funktionen anzeigen, mit der Datei als Input.

Sie können die Datei "Logic Path Graph" mit einer der folgenden Methoden herunterladen:

- Klicken Sie auf der Seite **Analysis Results** (Analyseergebnisse) (**Analyse** | **Analysis Results**)auf , und wählen Sie **Logic Path Graph** (Logisches Pfaddiagramm) aus. Laden Sie dann die Datei "<file name>_logicpath.gml" herunter. Zum Verwenden dieser Option müssen Sie **Logic Path Graph** im entsprechenden Analyseprofil aktiviert haben.
- Nachdem Sie auf geklickt haben, wählen Sie **Complete Results** (Vollständige Ergebnisse) aus. Laden Sie die ZIP-Datei "<sample_name>" herunter. Die ZIP-Datei enthält die gleiche Datei "<file name>_logicpath.gml" im AnalysisLog-Ordner. Der ZIP-Bericht enthält die Datei "<file name>_logicpath.gml", ungeachtet dessen, ob Sie die Option **Logic Path Graph** (Logisches Pfaddiagramm) im entsprechenden Analyseprofil aktiviert haben.

In diesem Abschnitt wird der yWorks yEd Graph Editor verwendet, um zu erklären, wie die GML-Datei zu verwenden ist. Sie müssen im yEd Graph Editor zunächst den Routing-Stil festlegen. Wenn Sie dies einmal getan haben, wird die Einstellung für die künftige Verwendung gespeichert.

1 Wählen Sie im yEd Graph Editor **Layout** | **Hierarchical (Hierarchisch)** aus.

2 Wählen Sie im Dialogfeld **Incremental Hierarchic Layout** (Inkrementell hierarchisches Layout) die Registerkarte **Edges** (Kanten) aus, und wählen Sie aus der Dropdown-Liste **Routing Style** (Routing-Stil) **Polyline** (Hilfslinie) aus.

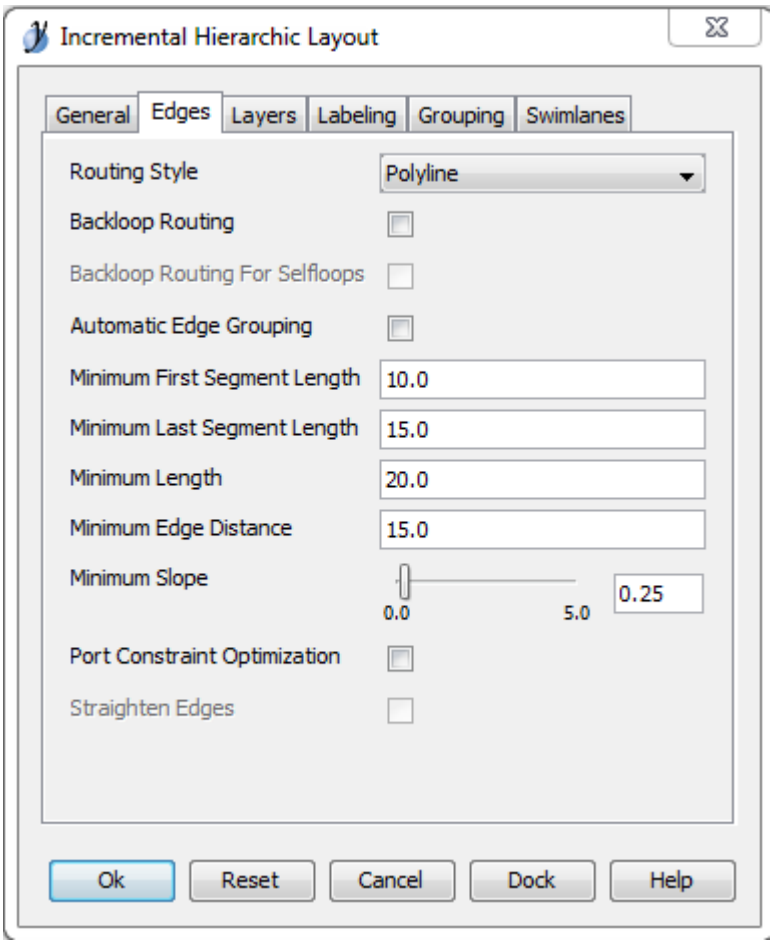


Abbildung 7-13 Konfigurieren des Routing-Stils im yEd Graph Editor

3 Klicken Sie auf **OK**.

Wenn Sie die Datei "<file name>_logicpath.gml" im yEd Graph Editor öffnen, könnten Sie am Anfang viele rechteckige Kästchen sehen, die sich überlappen, oder ein einzelnes rechteckiges Kästchen wie im folgenden Beispiel.

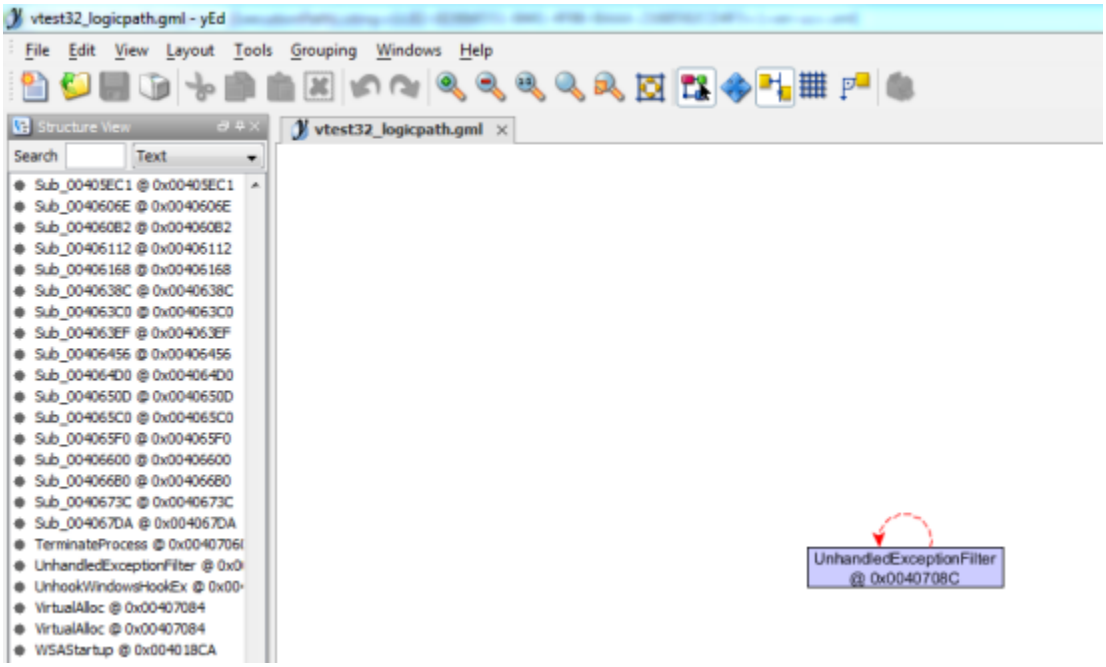


Abbildung 7-14 Geöffnete Datei "<file name>_logicpath.gml"

Wählen Sie im yEd Graph Editor **Layout** | **Hierarchical (Hierarchisch)** aus.

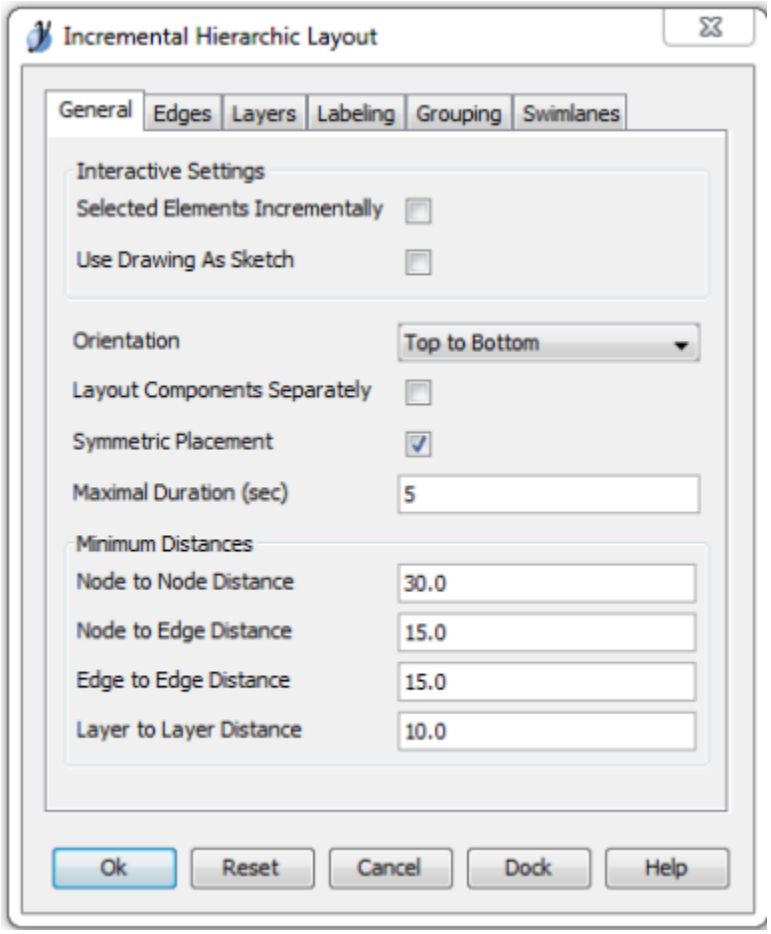


Abbildung 7-15 Dialogfeld "Incremental Hierarchic Layout"

Klicken Sie im Dialogfeld **Incremental Hierarchic Layout** (Inkrementell hierarchisches Layout) auf **OK**, ohne die Standardeinstellungen zu ändern. Im folgenden Beispiel sehen Sie das vollständige Layout der Beziehung aller Subroutinen, die während des statischen Disassembly-Vorgangs erkannt wurden.

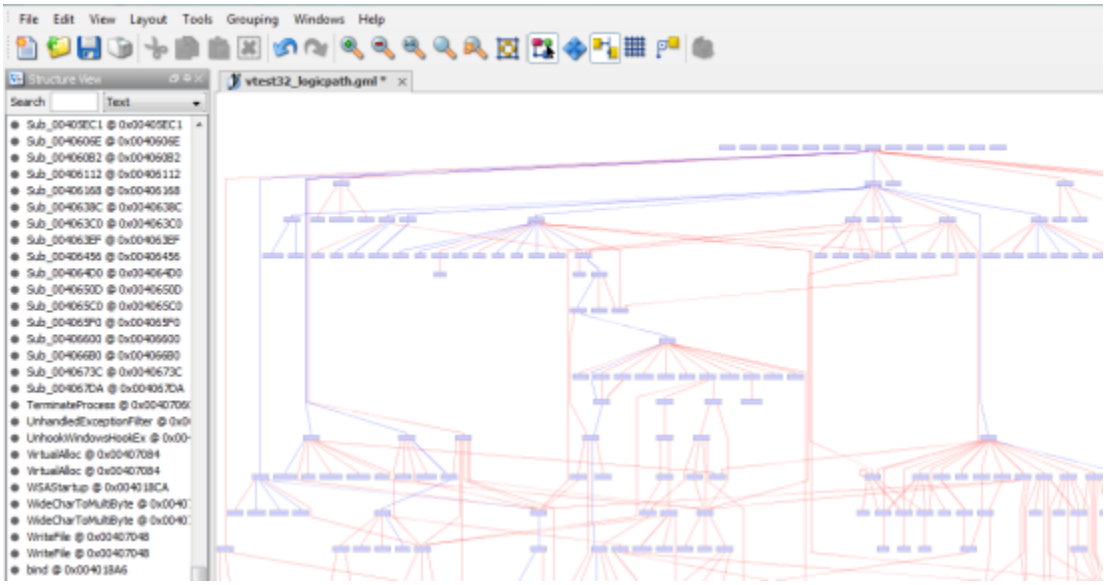


Abbildung 7-16 Layout der Subroutinen-Beziehungen

Das Diagramm stellt eine Übersicht über die Komplexität der Probe dar, wie an den Querverweisen der Funktionsaufrufe ersichtlich wird. Die folgende vergrößerte Abbildung zeigt mehr Details zu den Funktionsnamen und ihren Adressen.

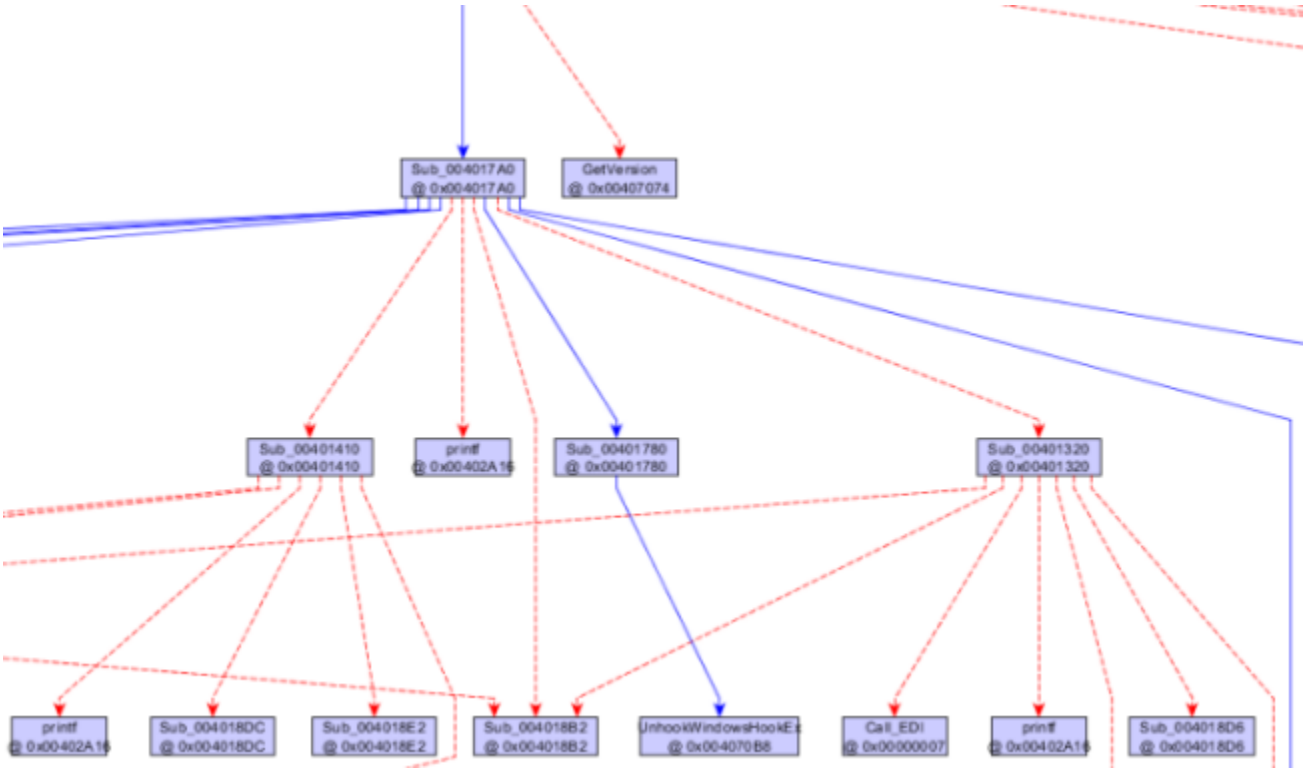


Abbildung 7-17 Vergrößerung des Layouts

Der ausgeführte Pfad wird durch zwei Farben angezeigt. Die roten Strichlinien zeigen den nicht ausgeführten Pfad und die durchgängig blauen Linien den ausgeführten Pfad.

Dem vorangegangenen Steuerdiagramm zufolge wurde die Subroutine (Sub_004017A0) unter der virtuellen Adresse 0x004017A0 ausgeführt und wird mit einer durchgängig blauen Linie angezeigt, die auf das Kästchen "Sub_004017A0" verweist. Die Subroutine (GetVersion]) wurde jedoch nicht aufgerufen, da nur eine rote Strichlinie darauf zeigt.

Die Subroutine "Sub_004017A0" führte elf Aufrufe aus, da elf Linien von diesem Kästchen ausgehen. Sieben von diesen elf Aufrufen wurden während der dynamischen Analyse ausgeführt. Ein Aufruf erfolgte für "Sub_00401780", da eine durchgängig blaue Linie von "Sub_004017A0" auf "Sub_00401780" zeigt. Aufrufe von "Sub_00401410", "printf", "Sub_00401882" und "Sub_00401320" wurden nicht ausgeführt und werden mit roten Strichlinien angezeigt, die auf sie verweisen.

Die Subroutine "Sub_00401780" führte nur einen einzigen Aufruf aus, da nur eine Linie von diesem Kästchen ausgeht. Der Aufruf erfolgte während der dynamischen Analyse.

User API-Protokoll

Die User API-Protokolle sind in verschiedenen Dateien enthalten.

- Die LOG-Datei enthält die Windows-DLL-API-Aufrufe auf Benutzerebene durch die analysierte Datei während der dynamischen Analyse. Wählen Sie zum Anzeigen dieser Datei in der McAfee Advanced Threat Defense-Web-Anwendung **Analyse** | **Analysis Results (Analyseergebnisse)** aus. Klicken Sie anschließend auf  und wählen Sie **User API-Protokoll** (User API-Protokoll) aus. Klicken Sie alternativ auf  , und wählen Sie dann **Complete Results** (Vollständige Ergebnisse) aus. Laden Sie die ZIP-Datei "<sample_name>" herunter. Die ZIP-Datei enthält dieselben Informationen wie die Datei "<sample name>.log" im AnalysisLog-Ordner. Folgendes ist in der LOG-Datei enthalten:
  - Ein Datensatz der System-DLL-API-Aufrufsequenzen
  - Eine Adresse, die der ungefähren Aufrufadresse entspricht, von der der DLL-API-Aufruf ausgeführt wurde
  - Optionale Eingabe- und Ausgabeparameter und Rückgabewert für wichtige System-DLL-API-Aufrufe
- Im Folgenden sind die Dateien aufgeführt, die die dynamischen Ausführungsprotokolle enthalten. Alle Dateien sind in der ZIP-Datei "<sample name>" enthalten.
  - <sample name>ntv.txt. Diese Datei enthält die Windows Zw-Version der nativen Systemdienst-API-Aufrufsequenz während der dynamischen Analyse. Der API-Name beginnt meist mit Zw, wie in "ZwCreateFile".
  - log.zip
  - dump.zip
  - dropfiles.zip
  - networkdrive.zip

Herunterladen der vollständigen Ergebnisse als ZIP-Datei

McAfee Advanced Threat Defense liefert eine detaillierte Analyse für jede gesendete Probe. Alle verfügbaren Berichte für eine analysierte Probe sind in einer ZIP-Datei enthalten, die Sie aus der McAfee Advanced Threat Defense-Web-Anwendung herunterladen können.

Vorgehensweise

1 Wählen Sie **Analyse** | **Analysis Results** (Analyseergebnisse) aus.

2 Klicken Sie auf der Seite **Analysis Results** (Analyseergebnisse) auf , und wählen Sie **Complete Results** (Vollständige Ergebnisse) aus.

Laden Sie die ZIP-Datei "<sample_name>" an den gewünschten Speicherort herunter. Die ZIP-Datei enthält die Berichte für jede Analyse. Die Dateien in der ZIP-Datei werden unter einem Standardnamen erstellt und gespeichert. Beachten Sie, dass die gesendete Probe im Format vtest32.exe ist. Die ZIP-Datei enthält die folgenden Ergebnisse:

- vtest32_summary.html (.json, .txt, .xml) – Diese ist identisch mit dem Übersichtsbericht der Analyse. In der ZIP-Datei sind vier Dateiformate für den gleichen Übersichtsbericht vorhanden. Die HTML- und TXT-Dateien sind hauptsächlich für Endbenutzer zur Überprüfung des Analyseberichts bestimmt. Die JSON- und XML-Dateien enthalten Verhaltenstags bekannter Malware für Programmierungsskripte, sodass Schlüsselinformationen extrahiert werden können.

  Ab einem Malware-Schweregrad von 3 sind IOC- und STIX.XML-Formate des Übersichtsberichts für die Analyse der Probe enthalten.

- vtest32.log – Diese Datei erfasst die DLL-API-Aufrufvorgänge auf Windows-Benutzerebene während der dynamischen Analyse. Sie müssen diese Datei sehr genau lesen, um die vollständige API-Aufrufsequenz sowie die Eingabe- und Ausgabeparameter zu verstehen. Sie ist mit dem User API-Protokoll identisch.

- vtest32ntv.txt – Diese Datei erfasst native API-Dienst-Aufrufvorgänge für Windows während der dynamischen Analyse.

- vtest32.txt – Diese Datei zeigt die PE-Header-Informationen der gesendeten Probe an.

- vtest32_detail.asm – Diese Datei ist mit dem Bericht "Disassembly Results" identisch. Sie enthält eine Reverse-Engineering-Disassembly-Liste der Probe, nachdem sie entpackt oder entschlüsselt wurde.

- vtest32_logicpath.gml – Diese Datei ist eine grafische Darstellung der Querverweise von Funktionsaufrufen, die während der dynamischen Analyse entdeckt wurden. Sie ist mit dem Bericht "Logic Path Graph" identisch.

- log.zip – Diese Datei enthält alle Laufzeit-Protokolldateien für alle Prozesse, die von der Probe während der dynamischen Analyse ausgeführt wurden. Wenn die Probe einen Ausgabetext für die Konsole generiert, wird dieser in der Datei ConsoleOutput.log erfasst, die in die ZIP-Datei log.zip gepackt wird. Verwenden Sie ein herkömmliches Dienstprogramm zum Entpacken, um den Inhalt aller Dateien innerhalb der ZIP-Datei log.zip anzuzeigen.

- dump.zip – Diese Datei enthält das Speicherabbild (dump.bin) des Binärcodes der Probe während der dynamischen Analyse. Die Datei ist kennwortgeschützt. Das Kennwort lautet *virus*.

- dropfiles.zip – Dies ist identisch mit dem Bericht "Dropped Files" auf der Seite **Analysis Results**. Die ZIP-Datei dropfiles.zip enthält alle Dateien, die von der Probe während der dynamischen Analyse erstellt oder geöffnet wurden. Sie ist ebenfalls kennwortgeschützt. Das Kennwort lautet *virus*.

McAfee Advanced Threat Defense gewährt Ihnen keinen Zugriff auf die Original-Probedateien, die analysiert wurden. Bei einer Integration in Network Security Platform können Sie die Option **Save File** (Datei speichern) in der erweiterten Malware-Richtlinie verwenden, um Proben zu archivieren. Beachten Sie jedoch, dass die Sensor-Kapazität für den gleichzeitigen Datei-Scan bei aktivierter Option **Save File** reduziert ist. Weitere Details finden Sie im aktuellen *Network Security PlatformIPS Administration Guide*.

Download der Originalprobe

Mithilfe von McAfee Advanced Threat Defense können Benutzer die gesendeten Originaldateien herunterladen. Alle gesendeten Proben sind in einer ZIP-Datei enthalten, die Sie wie folgt herunterladen können.

Vorgehensweise

1. Wählen Sie **Verwalten** | **Benutzerverwaltung**.
2. Wählen Sie auf der Seite **Benutzerverwaltung** Ihr Benutzerprofil aus.
3. Aktivieren Sie die Option **Sample Download** (Download von Proben).
4. Wählen Sie **Analysis Results** (Analyseergebnisse) aus, klicken Sie auf das Symbol **Berichte**, und wählen Sie dann **Original Sample** (Originalprobe) aus.
5. Speichern Sie die komprimierte Datei **atd_sample.zip** auf Ihrem lokalen Computer.
6. Extrahieren Sie den Inhalt von **atd_sample.zip** unter Verwendung des Kennwortes `infected`.

Arbeiten mit dem McAfee Advanced Threat Defense-Dashboard

Wenn Sie über einen Client-Browser auf McAfee Advanced Threat Defense zugreifen, wird das McAfee Advanced Threat Defense-Dashboard angezeigt. Sie können die folgenden Monitore im McAfee Advanced Threat Defense-Dashboard anzeigen:

- VM Creation Status – Zeigt den Status für Analyse-VMs an, die erstellt werden.
- File Counters – Zeigt einen Status von analysierten Dateien an.
- Top 5 URLs Analyzed by GTI – Listet fünf der schädlichsten URLs auf, die durch die GTI analysiert werden.
- Top 5 URLs – Listet fünf der schädlichsten URLs auf, die analysiert werden.
- Profile Usage – Führt die Anzahl der unter verschiedenen Analyseprofilen analysierten Dateien auf.
- Files Analyzed by Engine – Stellt den Schweregrad und die Anzahl der von der GAM, der GTI und dem Sandkasten analysierten Dateien bereit.
- Top 10 File Types by Volume – Stellt eine Ansicht der zehn häufigsten Dateien von unterschiedlichen Typen bereit, die analysiert werden.
- Top 5 Recent Malware by Filename – Listet die fünf gefährlichsten Malware-Dateien in Ihrem Netzwerk auf, geordnet nach Dateinamen.
- Top 10 Malware by Threat Name – Listet die zehn gefährlichsten Malware-Dateien in Ihrem Netzwerk auf, geordnet nach Bedrohungsnamen.
- System Health – Gibt Details zum Systemzustand der McAfee Advanced Threat Defense Appliance an.
- System Information – Gibt die Versionsnummern für die Softwarekomponenten der McAfee Advanced Threat Defense Appliance an.

Vorgehensweise

1 Klicken Sie auf **Dashboard**, um die Monitore anzuzeigen.

2 Legen Sie die Kriterien für die auf den Monitoren angezeigten Daten fest.

a Legen Sie den Zeitraum für die auf den Monitoren angezeigten Informationen fest.

Sie können beispielsweise auswählen, die Informationen für die letzte halbe Stunde anzuzeigen. Standardmäßig werden Daten für die vergangenen 14 Tage angezeigt. Dieses Feld hat keine Auswirkung auf die Monitore für Systemzustand und Systeminformationen.

b Zum Aktualisieren der Monitore klicken Sie auf .

c Klicken Sie auf , um die Dashboard-Einstellungen zu bearbeiten.

Tabelle 7-11 Dashboard-Einstellungen

Option	Beschreibung
Monitors (Monitore)	Wählen Sie die Monitore aus, die Sie im Dashboard sehen möchten.
Automatic Refresh (Automatische Aktualisierung)	Legen Sie fest, wie oft sich das Dashboard automatisch aktualisieren soll. Wenn Sie das Dashboard nur manuell aktualisieren möchten, wählen Sie **Disabled** (Deaktiviert). Wenn Sie das Dashboard aktualisieren möchten, klicken Sie auf . Damit können Sie den Snapshot des Dashboards zu einem bestimmten Zeitpunkt anzeigen.
Layout	Legen Sie die Spaltenanzahl im Dashboard fest.
OK	Klicken Sie auf diese Schaltfläche, um die Dashboard-Einstellungen zu speichern und zu übernehmen.
Abbrechen	Klicken Sie auf diese Schaltfläche, um die zuletzt gespeicherten Einstellungen zu behalten.

d Klicken Sie auf , um die Dashboard-Einstellungen zu speichern.

3 Wahlweise können Sie die Anzeigeeinstellungen für jeden Monitor festlegen.

- Zum Einklappen eines Monitors klicken Sie auf .
- Zum Ausblenden eines Monitors klicken Sie auf .
- Um das Anzeigeformat eines Monitors zu ändern, klicken Sie auf .

Malware-Analysemonitore

Nachfolgend sind die Monitore für die Malware-Analyse beschrieben.

File Counters

Dieser Monitor zeigt den Analysestatus der während des festgelegten Zeitraums übermittelten Dateien an. Beispiel: Wenn Sie im Dashboard für die Daten beim Zeitraum die letzten 5 Minuten festgelegt haben, wird im Monitor für diesen Zeitraum angezeigt, für wie viele Dateien die Analyse abgeschlossen

wurde, wie viele gerade analysiert werden und bei wie vielen die Analyse noch aussteht. Falls Sie für diesen Monitor die Anzeige als gestapeltes Balkendiagramm aktiviert haben, wird auch der Schweregrad der Dateien angegeben.

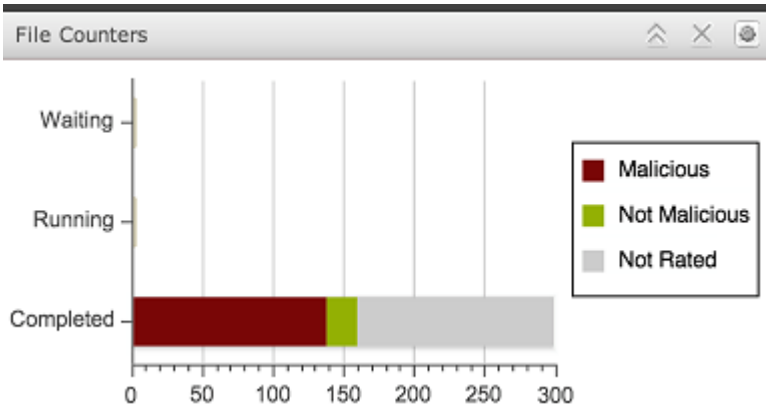


Abbildung 7-18 Monitor "File Counters"

- Der Schweregrad wird anhand verschiedener Farben angegeben.
- Um die Dateien mit einem bestimmten Schweregrad auszublenden, klicken Sie in der Legende auf den entsprechenden Schweregrad. Wenn Sie sich zum Beispiel auf bösartige Dateien konzentrieren möchten, klicken Sie in der Legende auf **Not Malicious** (Nicht bösartig) und **Not Rated** (Nicht bewertet). Daraufhin wird im Diagramm nur Malware mit hohem Schweregrad mit ausstehendem, aktivem oder abgeschlossenem Status angezeigt. Um das gesamte Diagramm erneut anzuzeigen, klicken Sie erneut auf **Not Malicious** und **Not Rated**.
- Bewegen Sie den Mauszeiger über einen Balken im Diagramm, um zu sehen, aus wie vielen Dateien der Balken besteht.

Dieser Monitor verfügt über eine Drilldown-Funktion. Wenn Sie mit dem Mauszeiger auf einen bestimmten Balken klicken, öffnet Advanced Threat Defense die Seite **Analysis Results** (Analyseergebnisse), auf der die Datensätze nach dem gewählten Balken sortiert angezeigt werden.

Top 10 File Types by Volume

Dieser Monitor zeigt die Anzahl der 10 häufigsten Dateitypen basierend auf ihrem Volumen an. Im Tabellenformat wird der Prozentsatz je Dateityp angezeigt. Im Diagramm ist auch die Anzahl der bösartigen (Malicious), nicht bösartigen (Not Malicious) und der nicht bewerteten Dateien (Not Rated) zu sehen.

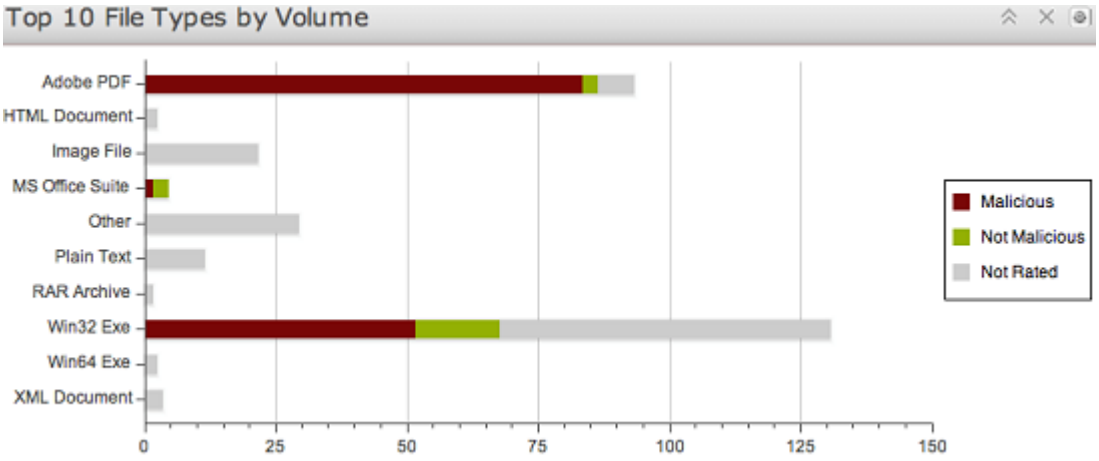


Abbildung 7-19 Monitor "Top 10 File Types by Volume"

- Die bösartigen, nicht bösartigen und nicht bewerteten Dateien werden in verschiedenen Farben dargestellt.
- Um die bösartigen oder nicht bösartigen Dateien auszublenden, klicken Sie in der Legende auf den entsprechenden Schweregrad.
- Bewegen Sie den Mauszeiger über einen Balken im Diagramm, um zu sehen, aus wie vielen Dateien der Balken besteht.

Dieser Monitor verfügt über eine Drilldown-Funktion. Wenn Sie mit dem Mauszeiger auf einen bestimmten Balken klicken, öffnet Advanced Threat Defense die Seite **Analysis Results** (Analyseergebnisse), auf der die Datensätze nach dem gewählten Balken sortiert angezeigt werden.

Profile Usage

Dieser Monitor stellt dar, wie oft jedes Analyseprofil für die Dateianalyse benutzt wurde.

Profile Usage

Analyzer Profile	No. of Files
File type not supported	5
StaticAnalysis	10
android	1
win7sp1x64	1
winXPsp3	70

Abbildung 7-20 Monitor "Analyzer Profile Usage"

Top 5 Recent Malware by File Name

In diesem Monitor sehen Sie die Namen der fünf bösartigsten in Ihrem Netzwerk erkannten Dateien. Die schädlichsten sind oben in der Liste aufgeführt. Aufgrund dieser Informationen können Sie beispielsweise im Web weitere Recherchen zu diesen Dateien durchführen.

- Die Malware-Dateien sind in absteigender Reihenfolge nach ihrem Schweregrad sortiert.
- In der ersten Spalte werden die Dateinamen angezeigt. In der zweiten Spalte wird der Schweregrad angezeigt.

Top 5 Recent Malware by Filename

File Name	Severity
mal_sample.exe	Very High
테스트.pdf	Very High
MS09-072_MSWordRecordParsingBuff...	Very High
тест.pdf	Very High
테스트.pdf	Very High

Abbildung 7-21 Monitor "Top 5 Recent Malware by File Name"

Top 10 Malware by Threat Name

In diesem Monitor sehen Sie die zehn schädlichsten in Ihrem Netzwerk erkannten Malware-Dateien nach Bedrohungsnamen.

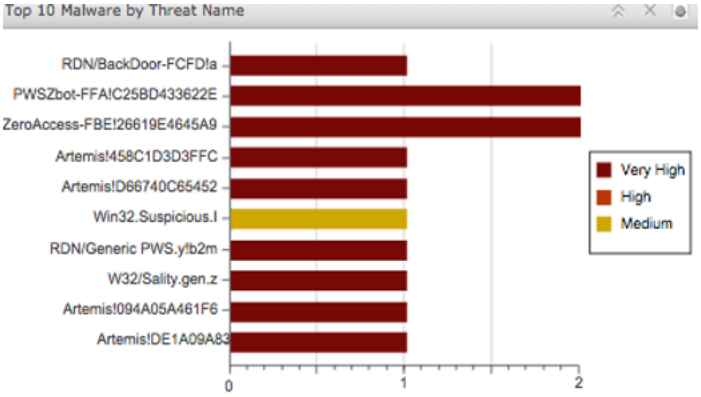


Abbildung 7-22 Top 10 Malware by Threat Name

Dieser Monitor verfügt über eine Drilldown-Funktion. Wenn Sie mit dem Mauszeiger auf einen bestimmten Balken klicken, öffnet Advanced Threat Defense die Seite **Analysis Results** (Analyseergebnisse), auf der die Datensätze nach dem gewählten Balken sortiert angezeigt werden.

Files Analyzed by Engine

In diesem Monitor sehen Sie den Schweregrad und die Anzahl der von der GAM, der GTI und dem Sandkasten analysierten Dateien.

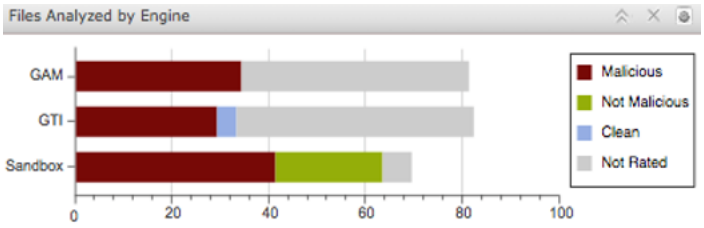


Abbildung 7-23 Files Analyzed by Engine

Dieser Monitor verfügt über eine Drilldown-Funktion. Wenn Sie mit dem Mauszeiger auf einen bestimmten Balken klicken, öffnet Advanced Threat Defense die Seite **Analysis Results** (Analyseergebnisse), auf der die Datensätze nach dem gewählten Balken sortiert angezeigt werden.

Top 5 URLs Analyzed by GTI

In diesem Monitor sehen Sie die fünf schädlichsten von GTI analysierten URLs. Aufgrund dieser Informationen können Sie beispielsweise im Web weitere Recherchen zu diesen Dateien durchführen.

- Die Malware-Dateien sind in absteigender Reihenfolge nach ihrem Schweregrad sortiert.
- In der ersten Spalte werden die Dateinamen angezeigt. In der zweiten Spalte wird der Schweregrad angezeigt.

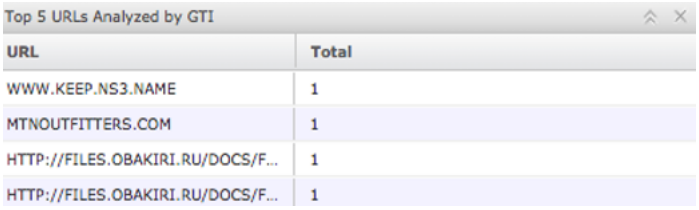


Abbildung 7-24 Top 5 URLs Analyzed by GTI

Top 5 URLs

In diesem Monitor sehen Sie die Namen der fünf bösartigsten in Ihrem Netzwerk erkannten Dateien. Die schädlichsten sind oben in der Liste aufgeführt. Aufgrund dieser Informationen können Sie beispielsweise im Web weitere Recherchen zu diesen Dateien durchführen.

- Die Malware-Dateien sind in absteigender Reihenfolge nach ihrem Schweregrad sortiert.
- In der ersten Spalte werden die Dateinamen angezeigt. In der zweiten Spalte wird der Schweregrad angezeigt.



Abbildung 7-25 Top 5 URLs

Monitor "VM Creation Status"

Dieser Monitor zeigt die Farbe auf Grundlage des Status der VM-Erstellung an. Nachstehend wird der Farbcode angegeben:

Wird ausgeführt – Gelb

Fehlgeschlagen – Rot

Erfolgreich – Grün

Im Folgenden finden Sie ein Beispiel für den **Monitors "VM Creation Status"**, wenn der Status der VM-Erstellung "Erfolgreich" ist:

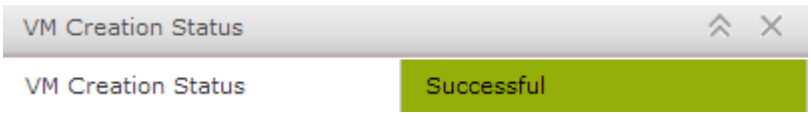


Abbildung 7-26 Monitor "VM Creation Status"

McAfee Advanced Threat Defense-Leistungsmonitore

Folgende Monitore stehen für die Überwachung der McAfee Advanced Threat Defense Appliance-Leistung zur Verfügung:

System Health (Systemzustand)

Dieser Monitor zeigt den Status der McAfee Advanced Threat Defense Appliance in einer Tabelle an.

- System Health (Systemzustand) – Zeigt an, ob sich das System in einem guten Status befindet. Grün steht für einen guten Status und Rot für einen schlechten.
- DNS Status (DNS-Status) – Gibt den Verbindungsstatus zwischen Advanced Threat Defense und den konfigurierten DNS-Servern an. Wenn Advanced Threat Defense eine Verbindung zum bevorzugten und alternativen DNS-Server herstellen kann, wird der DNS-Status *Fehlerfrei* in Grün angezeigt. Kann Advanced Threat Defense keine Verbindung zum bevorzugten DNS-Server herstellen, wird der DNS-Status *Kritisch* in Rot angezeigt. Wenn die Advanced Threat Defense mit keinem bevorzugten DNS-Server verbunden ist, dann wird der DNS-Status *Nicht konfiguriert* in Rot angezeigt.
- Uptime (Betriebszeit) – Die Anzahl der Stunden, die die Appliance durchgängig in Betrieb ist.
- CPU Load (CPU-Auslastung) – Die tatsächliche Systemauslastung. Beispiel: Eine CPU-Auslastung von 100 % gibt an, dass die CPU vollständig ausgelastet ist, und eine CPU-Auslastung von 125 % gibt an, dass die CPU vollständig ausgelastet ist und noch 25 % verarbeitet werden müssen.
- Memory Utilization (Speichernutzung) – Der Prozentsatz der derzeit genutzten Appliance-Speicherkapazität.
- Data Disk Space (Datenspeicherplatz) – Die Speicherkapazität der Appliance (in Terabyte) für die Speicherung von Probedaten, z. B. die Proben selbst und deren Berichtsdateien.
- Data Disk Available (Verfügbarer Datenspeicher) – Der derzeit verfügbare Speicherplatz (in Terabyte) für die Speicherung von Probedaten.



Abbildung 7-27 Monitor "System Health"

- System Disk Space (Systemspeicherplatz) – Die Datenträgerkapazität der Appliance für die Speicherung der Systemsoftwaredaten von McAfee Advanced Threat Defense.
- System Disk Available (Verfügbarer Systemspeicher) – Der derzeit verfügbare Speicherplatz für die Speicherung der Systemsoftwaredaten von McAfee Advanced Threat Defense.

System Information (Systeminformationen)

Dieser Monitor zeigt die Versionsnummern der Softwarekomponenten von McAfee Advanced Threat Defense an.

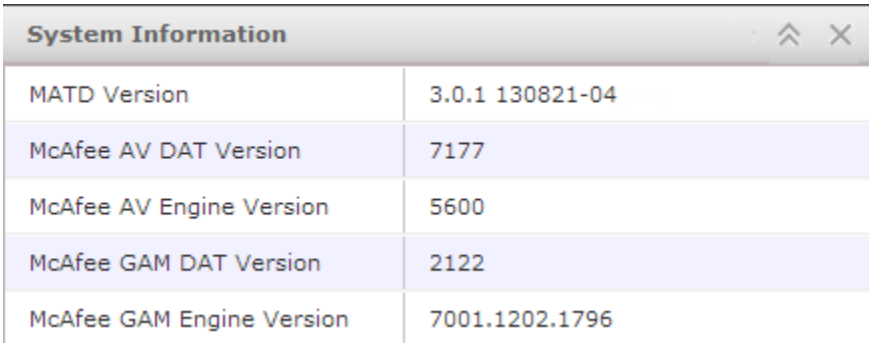


Abbildung 7-28 Monitor "System Information"

8

Clustering von McAfee Advanced Threat Defense Appliances

Wenn Sie in großem Umfang Dateien auf schädliche Inhalte analysieren müssen, können Sie zwei oder mehrere McAfee Advanced Threat Defense Appliances zu einem Cluster zusammenfassen. Auf diese Weise wird die Analyselast effizient auf die McAfee Advanced Threat Defense Appliances (Knoten) im Cluster aufgeteilt.

Mehrere Inline-Sensoren können Hunderte von Dateien pro Sekunde an eine McAfee Advanced Threat Defense Appliance senden. Im Blockiermodus wartet ein Sensor bis zu 6 Sekunden, bis McAfee Advanced Threat Defense eine Datei analysiert hat. Danach leitet der Sensor die Datei zum Zielendpunkt weiter. Durch das Clustering von McAfee Advanced Threat Defense Appliances zum Lastenausgleich kann eine deutlich schnellere Reaktionszeit von McAfee Advanced Threat Defense erreicht werden.

Inhalt

- *Erläuterungen zum McAfee Advanced Threat Defense-Cluster*
- *Voraussetzungen und Anmerkungen*
- *Netzwerkverbindungen für ein Advanced Threat Defense-Cluster*
- *Funktionsweise des Advanced Threat Defense-Clusters*
- *Konfigurieren eines Advanced Threat Defense-Clusters – Grundlegende Schritte*

Erläuterungen zum McAfee Advanced Threat Defense-Cluster

Clustering von McAfee Advanced Threat Defense Appliances ist eine ab Version 3.2.0 verfügbare Funktion. Um einen Cluster aus McAfee Advanced Threat Defense Appliances zu erstellen, benötigen Sie mindestens zwei funktionsfähige McAfee Advanced Threat Defense Appliances. Identifizieren Sie unter diesen McAfee Advanced Threat Defense Appliances die primäre McAfee Advanced Threat Defense Appliance. Alle anderen McAfee Advanced Threat Defense Appliances agieren als sekundäre Appliance. Ab Version 3.4.2 wird ein Knoten, der sich in demselben L2-Netzwerk wie die primäre McAfee Advanced Threat Defense Appliance befindet, direkt als Sicherungsknoten hinzugefügt. Dieser wird als primärer Knoten aktiviert, falls der eigentliche primäre Knoten ausfällt. Ein sekundärer Knoten kann nicht als Sicherungsknoten eingesetzt werden. Sie verwenden die Web-Anwendung des primären Knotens, um diese McAfee Advanced Threat Defense Appliances zu integrieren und den Cluster zu bilden. In einem Cluster wird jede McAfee Advanced Threat Defense Appliance als Knoten bezeichnet.

Der primäre Knoten oder die primäre McAfee Advanced Threat Defense Appliance agieren als externe Schnittstelle für das Cluster. Das heißt, dass der primäre Knoten in Bezug auf die Konfiguration und die Einsendung von Dateien virtuell mit der IP-Adresse des Clusters verknüpft ist. Die integrierten Produkte und Benutzer greifen auf den primären Knoten zu, um Dateien zur Analyse zu senden und die Ergebnisse und Berichte abzurufen. Der primäre Knoten fungiert auch als Vorlage und Steuerzentrale für das Cluster. Er ist für den Lastenausgleich von Dateien unter allen Knoten verantwortlich und ruft die Berichte für analysierte Dateien ab. Ist ein Sicherungsknoten im Cluster vorhanden, dann müssen diese integrierten Produkte mit der Cluster-IP-Adresse konfiguriert werden.

Wie bereits erwähnt, dient das Clustering von McAfee Advanced Threat Defense Appliances dem Lastenausgleich von Dateien. Es gewährleistet außerdem eine hohe Verfügbarkeit sekundärer Knoten.

Fällt der primäre Knoten aus irgendeinem Grund aus, übernimmt der Sicherungsknoten dessen Verantwortung sowie die Cluster-IP-Adresse des primären Knotens. Nach der Reaktivierung wartet der primäre Knoten in der Funktion des Sicherungsknotens, bis der eigentliche Sicherungsknoten ausfällt. Der Sicherungsknoten empfängt und analysiert die Proben jederzeit wie alle anderen Knoten.

Voraussetzungen und Anmerkungen

- In einem Cluster können sich maximal 10 Knoten befinden, einschließlich des primären Knotens.
- Es wird empfohlen, dass Sie die ETH-0-Schnittstellen (Verwaltungsports) der McAfee Advanced Threat Defense Appliances für die Cluster-Kommunikation verwenden. Für eine optimale Leistung müssen sich die ETH-0-Schnittstellen aller Knoten außerdem in demselben Schicht-2-Netzwerk befinden.

  Informationen zum Auffinden der ETH-0-Schnittstellen in Ihrer Appliance finden Sie unter Überprüfen der Lieferung auf Seite 22.
- Die Knoten müssen in Bezug auf folgende Aspekte homogen sein:
  - McAfee Advanced Threat Defense-Softwareversion. Die Softwareversionen aller Knoten müssen genau übereinstimmen.
  - Analyse-VMs. Alle Knoten müssen dieselben Analyse-VMs haben.

    Stellen Sie vor dem Konfigurieren des Clusters sicher, dass die VM-Profile aller Knoten des Clusters übereinstimmen. Sämtliche Einstellungen der VM-Profile, einschließlich des VM-Profilnamens, müssen bei allen Knoten identisch sein.

    Wenn Sie ein neues VM-Profil erstellen oder ein vorhandenes nach der Erstellung des Clusters ändern, bedenken Sie, dass Änderungen an einem VM-Profil nicht automatisch auf alle Knoten angewendet werden. Lösen Sie zunächst das Cluster auf. Nehmen Sie dann manuell die Änderungen für jeden Knoten einzeln vor. Wenn Sie ein neues VM-Profil erstellen, müssen Sie es zunächst für alle Knoten erstellen, bevor Sie das neue VM-Profil in einem der Analyseprofile auswählen. Wenn Sie ein vorhandenes VM-Profil ändern möchten, müssen Sie diese Änderung sofort auch für alle anderen Knoten vornehmen. Erstellen Sie nun das Cluster neu.
  - Die VM-Profile aller Knoten müssen genau übereinstimmen.
  - Es wird empfohlen, dass DAT- und Scan-Modul-Versionen der McAfee Anti-Malware Engine in allen Knoten übereinstimmen.
  - Es wird empfohlen, dass DAT- und Scan-Modul-Versionen der McAfee Gateway Anti-Malware Engine in allen Knoten übereinstimmen.

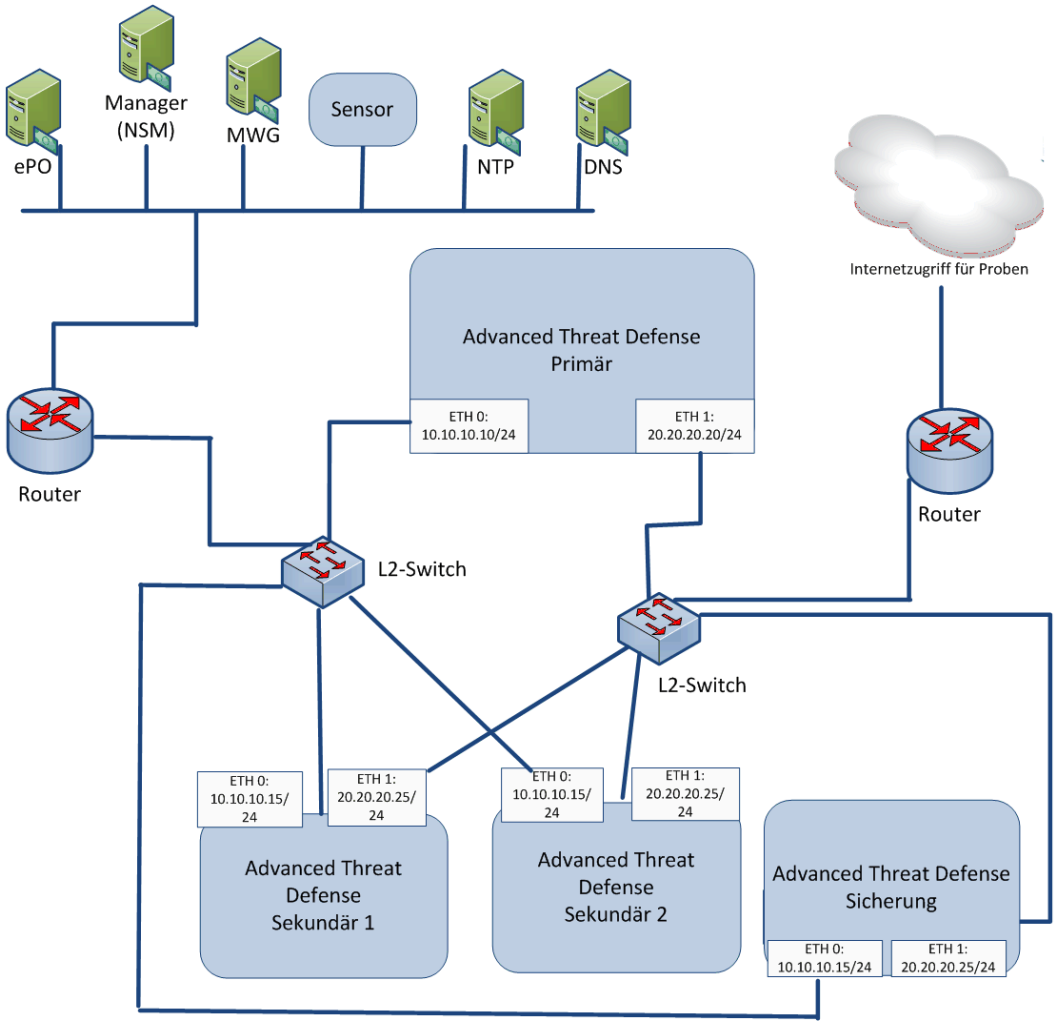
- Die Knoten können in Bezug auf folgende Aspekte heterogen sein:
  - Hardware. Das heißt, dass Sie ein Cluster aus einer Kombination aus ATD-3000- und ATD-6000-Appliances erstellen können.
  - FIPS-Konformität. Unabhängig davon, ob es sich um primäre oder sekundäre Knoten handelt, können sich einige Knoten im FIPS-Modus und der Rest im Nicht-FIPS-Modus befinden.
- Verwenden Sie die IP-Adresse des primären Knotens zum Einsenden von Dateien und zur Integration in andere Produkte, z. B. Network Security Platform und Web Gateway. Der primäre Knoten oder die primäre McAfee Advanced Threat Defense Appliance agieren als externe Schnittstelle für das Cluster. Das heißt, dass der primäre Knoten in Bezug auf die Konfiguration und die Einsendung von Dateien virtuell mit der IP-Adresse des Clusters verknüpft ist. Wenn Sie Network Security Platform, Web Gateway und Email Gateway in die sekundären Knoten integrieren, funktionieren diese Knoten wie eigenständige McAfee Advanced Threat Defense Appliances. Ist ein Sicherungsknoten im Cluster vorhanden, dann müssen diese integrierten Produkte mit der Cluster-IP-Adresse konfiguriert werden.

  Die Integration eines McAfee Advanced Threat Defense-Clusters in Email Gateway wird ab Version 3.4.2 unterstützt.

- Sollte der primäre Knoten ausfallen, übernimmt der Sicherungsknoten. Der Sicherungsknoten muss sich im selben L2-Netzwerk befinden wie der primäre Knoten.
- Benutzer können den Analysestatus und die Analyseergebnisse aller Knoten im Cluster über den aktiven Knoten, d. h. den primären oder den Sicherungsknoten, sehen.

Netzwerkverbindungen für ein Advanced Threat Defense-Cluster

Abbildung 8-1 Beispiel für die Bereitstellung eines Advanced Threat Defense-Clusters



Im oben abgebildeten Beispiel sind die ETH-0-Schnittstellen aller Knoten mit dem selben Switch (L2-Netzwerk) verbunden. Die ETH-0-Schnittstelle des primären Knoten agiert als Managementschnittstelle des Clusters, während die ETH-0-Schnittstellen des sekundären und des Sicherungsknotens zum Informationsaustausch mit dem primären Knoten dienen. Der Sicherungsknoten dient als ein sekundärer Knoten, bis der primäre Knoten aus irgendeinem Grund ausfällt und der Sicherungsknoten die Rolle des aktiven primären Knotens übernimmt. Der primäre Knoten führt den Lastenausgleich der auf der ETH-0-Schnittstelle empfangenen Dateien unter den sekundären Knoten nach dem Round-Robin-Verfahren durch. Er überträgt die durch den sekundären Knoten zu analysierenden Dateien über die ETH-0-Schnittstelle und verwendet diese auch zum Abrufen der Ergebnisse. Werden über den primären Knoten Änderungen an der Clusterkonfiguration vorgenommen, wird die Synchronisierung der sekundären Knoten und des Sicherungsknotens über die ETH-0-Schnittstelle durchgeführt.

In diesem Beispiel wird ETH-1 zur Bereitstellung von Netzwerkzugriff für Malware verwendet, die auf den Analyse-VMs ausgeführt wird. Dadurch wird der durch Malware verursachte Netzwerkdatenverkehr vom Produktionsnetzwerk, mit dem die ETH-0-Schnittstellen verbunden sind, isoliert.

Funktionsweise des Advanced Threat Defense-Clusters

Beachten Sie Folgendes: Wenn Sie ein Cluster für Advanced Threat Defense Appliances erstellen, fungiert der primäre Knoten als Vorlage und Control Center für das gesamte Cluster. Nachdem Sie das Cluster definiert haben, können Sie das Cluster mithilfe des primären Knotens konfigurieren.

Der Sicherungsknoten verhält sich wie ein sekundärer Knoten für alle Konfigurationsprozesse.

Zu Erklärungszwecken kann die gesamte Advanced Threat Defense-Konfiguration folgendermaßen klassifiziert werden:

- Synchronisierte Konfiguration – Bestimmte Konfigurationen sind nur mithilfe des primären Knotens möglich. Wenn Sie diese Konfigurationen speichern, sendet der primäre Knoten einen Snapshot seiner aktuellen Konfiguration in Dateiform an alle sekundären Knoten. Die sekundären Knoten speichern diese Einstellungen in ihrer Datenbank. Dieser Synchronisierungsprozess hat keine Auswirkungen auf die Dateianalyse-Funktion einer Advanced Threat Defense Appliance.

  Der primäre Knoten verfügt über die aktuelle Version der Konfigurationsdatei. Wenn die Versionen der Konfigurationsdatei des primären und sekundären Knotens nicht übereinstimmen, überträgt der primäre Knoten die Konfigurationsdatei mithilfe von Push automatisch an den sekundären Knoten.

  Die folgenden Konfigurationen werden automatisch zwischen allen Knoten synchronisiert:

  - Analyseprofile
  - Benutzerverwaltung
  - McAfee ePO/DXL-Integrationsinformationen
  - Proxy-Einstellungen
  - DNS-Einstellungen
  - Die Systemzeit basierend auf den Einstellungen auf der Seite **Date and Time Settings** (Datums- und Uhrzeiteinstellungen). Wenn Sie die Zeit manuell ändern, werden alle Knoten auf diese Zeit gesetzt. Wenn Sie NTP-Server konfigurieren, werden dieselben NTP-Server für alle Knoten verwendet. Allerdings wird die Zeitzone nicht synchronisiert.

  Die Seiten der Web-Anwendung für die oben genannten Konfigurationen sind sowohl für sekundäre Knoten als auch für Sicherungsknoten deaktiviert.

- Nicht synchronisierte Konfiguration – Folgende Elemente werden nicht automatisch synchronisiert. Konfigurieren Sie diese über die einzelnen Knoten.
  - Advanced Threat Defense-Softwareversion
  - Analyse-VMs

Stellen Sie vor dem Konfigurieren des Clusters sicher, dass die VM-Profile aller Knoten des Clusters übereinstimmen. Sämtliche Einstellungen der VM-Profile, einschließlich des VM-Profilnamens, müssen bei allen Knoten identisch sein.

Wenn Sie ein neues VM-Profil erstellen oder ein vorhandenes nach der Erstellung des Clusters ändern, bedenken Sie, dass Änderungen an einem VM-Profil nicht automatisch auf alle Knoten angewendet werden. Lösen Sie zunächst das Cluster auf. Nehmen Sie dann manuell die Änderungen für jeden Knoten einzeln vor. Wenn Sie ein neues VM-Profil erstellen, müssen Sie es zunächst für alle Knoten erstellen, bevor Sie das neue VM-Profil in einem der Analyseprofile auswählen. Wenn Sie ein vorhandenes VM-Profil ändern möchten, müssen Sie diese Änderung sofort auch für alle anderen Knoten vornehmen. Erstellen Sie nun das Cluster neu.

- VM-Profile
- DAT- und Scan-Modul-Versionen der McAfee Anti-Malware Engine
- DAT- und Scan-Modul-Versionen der McAfee Gateway Anti-Malware Engine
- Whitelist- und Blacklist-Einträge
- Zeitzone
- Wenn Advanced Threat Defense als Cluster eingerichtet ist, verwendet jeder Knoten seinen eigenen Satz von YARA-Regeln. Das bedeutet, dass die von Ihnen im primären Knoten definierten YARA-Regeln nicht automatisch an die sekundären Knoten gesendet werden.

Mithilfe der CLI vorgenommene Konfigurationsänderungen werden nicht ausgetauscht. Sie müssen dieselben Änderungen für jeden Knoten einzeln vornehmen.

Wenn die sekundären Knoten als Teil eines Clusters behandelt werden, sind sie für Benutzer und integrierte Produkte transparent.

- Sie können eine sekundäre Advanced Threat Defense direkt für die Dateiübertragung und den Berichtsabruf verwenden. Sie können jedoch keinerlei synchronisierten Konfigurationen ändern.
- Zur Analyse gesendete Dateien und URLs werden zwecks Lastenausgleich verteilt.

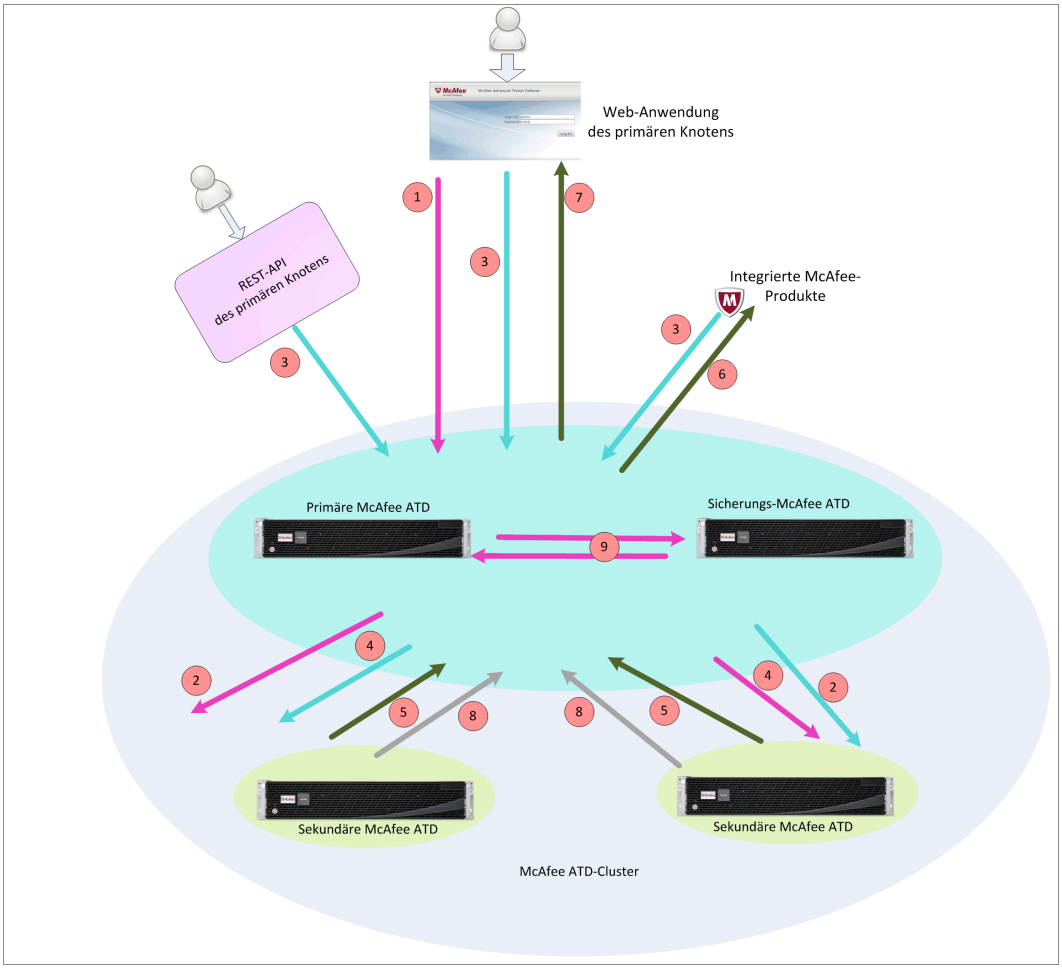


Abbildung 8-2 Advanced Threat Defense Appliances in einem Cluster

Positionszahl	Legende	Beschreibung
1		Sie greifen auf die Web-Anwendung des primären Knotens zu, um die synchronisierten Konfigurationen zu ändern.
2		Wenn Sie die Konfigurationsänderungen speichern, überträgt der primäre Knoten die aktuelle Konfiguration mithilfe von Push an alle sekundären Knoten. Alle Knoten verfügen demnach über dieselbe synchronisierte Konfiguration. In Version 3.4.2 kann der Benutzer auf die Cluster-IP-Schnittstelle zugreifen, um Konfigurationsänderungen vorzunehmen. Die Cluster-IP-Schnittstelle entspricht immer der Schnittstelle des aktiven Knotens.
3		Die Dateiübertragung zum Cluster erfolgt auf folgenden Wegen: • Sie senden die Dateien mithilfe der Web-Anwendung des primären Knotens zur Analyse. • Die Dateiübertragung zum primären Knoten erfolgt über dessen REST-APIs. • Die in Advanced Threat Defense integrierten McAfee-Produkte senden Dateien zur Analyse.
4		Der primäre Knoten verteilt die Dateien unter den Mitgliedsknoten (einschließlich dem primären Knoten).
5		Integrierte McAfee-Produkte wie der Network Security Manager fragen den primären Knoten nach Analyseberichten ab. Darüber hinaus zeigt der primäre Knoten den Status und die Ergebnisse aller vom Cluster analysierten Dateien an. Daher ruft der primäre Knoten die Analyseergebnisse von den sekundären Knoten ab.
6		Der primäre Knoten stellt den integrierten McAfee-Produkten die Berichte zur Verfügung.
7		Sie können den Status und die Ergebnisse aller vom Cluster analysierten Dateien über den primären Knoten anzeigen. Ebenfalls über den primären Knoten können Sie die Analyseberichte von direkt an einen sekundären Knoten gesendeten Dateien anzeigen.
8		In regelmäßigen Abständen senden die sekundären Knoten ein Heartbeat-Signal mit Informationen zum Zustand und Status des jeweiligen sekundären Knotens an den primären Knoten.
9		Die Sicherungs-Advanced Threat Defense übernimmt die Rolle der primären Advanced Threat Defense, wenn die eigentliche primäre Advanced Threat Defense ausfällt.

Wie werden die in einer ZIP-Datei enthaltenen Dateien von einem Advanced Threat Defense-Cluster analysiert?

Wenn Sie eine Datei oder URL senden, weist Advanced Threat Defense ihr eine eindeutige Auftrags-ID und eine Task-ID zu. Bei diesen IDs handelt es sich um inkrementelle Ganzzahlen. Wenn Sie eine ZIP-Datei senden, werden die Komponentendateien extrahiert und einzeln analysiert. Die Auftrags-ID der einzelnen Komponentendateien entspricht der der ZIP-Datei. Jedoch besitzen die Komponentendateien verschiedene Task-IDs.

Wenn Sie eine ZIP-Datei an ein Advanced Threat Defense-Cluster senden, identifiziert der primäre Knoten den Knoten, an den die nächste Datei verteilt werden soll, und sendet dann die gesamte ZIP-Datei an diesen. Der Knoten, der die ZIP-Datei erhalten hat, extrahiert und analysiert die Komponentendateien. Dies gilt auch für ZIP-Dateien innerhalb einer ZIP-Datei.

- Sendet ein Sensor die ZIP-Datei, generiert Advanced Threat Defense einen kumulativen Bericht für die gesamte ZIP-Datei. Das bedeutet, dass je ZIP-Datei ein Bericht an den Manager gesendet wird, wenn dieser den Bericht abfragt. Für Web Gateway werden keine ZIP-Dateien unterstützt.
- Wenn Sie eine ZIP-Datei beispielsweise über dessen Web-Anwendung an den primären Knoten senden, werden für die Komponentendateien innerhalb der ZIP-Datei einzelne Berichte generiert.

Der primäre Knoten extrahiert dann die Komponentendateien der ZIP-Datei und verteilt sie zur Analyse an denselben Knoten. Der primäre Knoten fragt mithilfe der eindeutigen Task-ID beim entsprechenden sekundären Knoten den Analysestatus und die Analyseergebnisse ab.

Durchführen eines Upgrades der Advanced Threat Defense-Software für die Knoten in einem Cluster

Im Folgenden finden Sie die empfohlene Vorgehensweise für ein Upgrade der Advanced Threat Defense-Software für die Knoten in einem Cluster:

1. Wenn Sie zunächst ein Upgrade des primären Knotens durchführen, bricht das gesamte Cluster zusammen. Daher sollten Sie mit dem Upgrade der sekundären Knoten beginnen. Wenn die Softwareversion eines sekundären Knotens aktualisiert wird, verteilt der primäre Knoten keine Dateien an diesen sekundären Knoten.
2. Nachdem Sie ein Upgrade für mehr als 50 % der sekundären Knoten durchgeführt haben, können Sie den primären Knoten ebenfalls aktualisieren. Der primäre Knoten verteilt keine Dateien an die sekundären Knoten, die sich noch auf dem Stand der früheren Version befinden.
3. Führen Sie dann ein Upgrade der verbleibenden sekundären Knoten durch.



Der Sicherungsknoten verhält sich wie ein sekundärer Knoten für alle Software-Upgrade-Prozesse.



Wählen Sie **Datenbank zurücksetzen** nicht aus, wenn Sie ein Upgrade für einen Knoten durchführen. Wird diese Option für den primären Knoten ausgewählt, bricht das Cluster nach dem Upgrade zusammen. Wenn die Option **Datenbank zurücksetzen** für einen sekundären Knoten ausgewählt wird, wird nach dem Upgrade dessen Verbindung zum Cluster getrennt.

Prozessablauf für Network Security Platform

Stellen Sie sich ein Szenario vor, in dem sich ein Sensor zwischen den Endpunkten in Ihrem Netzwerk und dem Internet befindet. Dieser Sensor ist in ein Advanced Threat Defense-Cluster integriert, das aus 3 Advanced Threat Defense Appliances besteht.

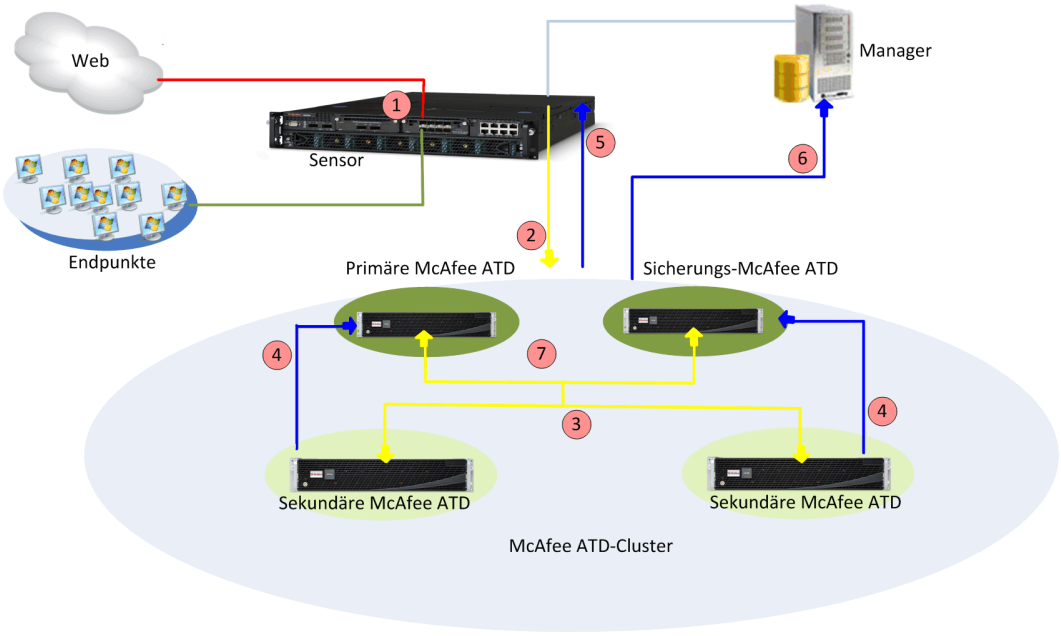


Abbildung 8-3 Network Security Platform integriert in ein Advanced Threat Defense-Cluster

Nummer	Beschreibung
1	Die Endpunkte versuchen, Dateien aus dem Internet herunterzuladen. Die Inline-Überwachungsports erkennen diese Aktivität.
2	Für eine gegebene Datei hält der Sensor die Weiterleitung des letzten Pakets an den Endpunkt zurück und übermittelt gleichzeitig die Dateipakete an die primäre Advanced Threat Defense zur Analyse. Zu diesem Zweck nutzen der Sensor und die primäre Advanced Threat Defense ihre Verwaltungsports.
3	Wenn die gesamte Datei bei der primären Advanced Threat Defense Appliance ist, verteilt diese die Datei an eine der Appliances im Cluster. Angenommen, die Datei wird an eine sekundäre Advanced Threat Defense Appliance gesendet. Die Mitglieder im Cluster nutzen ihre Verwaltungsports für die gesamte Kommunikation.
4	Die korrespondierende sekundäre Advanced Threat Defense antwortet mit einer Auftrags-ID an die primäre und beginnt mit der Analyse der Datei auf Grundlage des Benutzerprofils. Wenn die Datei durch statische Analyse erkannt wird, sendet die sekundäre Advanced Threat Defense das Malware-Ergebnis (Schweregrad) an die primäre Advanced Threat Defense.
5	• Wenn die Datei durch statische Analyse erkannt wird, sendet die primäre Advanced Threat Defense das Malware-Ergebnis, das sie von der sekundären Advanced Threat Defense erhalten hat, an den Verwaltungsport des Sensors. • Wenn die Datei dynamisch analysiert wird, erstellt der Sensor einen Informationshinweis im Echtzeit-Threat Analyzer. Dieser Informationshinweis wird standardmäßig auf automatische Bestätigung eingestellt, die Sie bei Bedarf deaktivieren können.

Nummer	Beschreibung
6	Der Sensor leitet die Auftrags-ID an den Manager weiter. Der Manager fragt beim Verwaltungsport der primären Advanced Threat Defense Appliance die Analyseberichte an. Die primäre Advanced Threat Defense extrahiert die Berichte aus der korrespondierenden Advanced Threat Defense Appliance auf Grundlage der Auftrags-ID. Anschließend leitet sie die Berichte zur Anzeige an den Manager weiter. Wird aufgrund der dynamischen Analyse festgestellt, dass die Datei bösartig ist, wird die Warnung im Echtzeit-Threat Analyzer entsprechend aktualisiert.
7	Die Sicherungs-Advanced Threat Defense übernimmt die Rolle der primären Advanced Threat Defense, wenn die eigentliche primäre Advanced Threat Defense ausfällt.

Prozessablauf für McAfee Web Gateway

Stellen Sie sich ein Szenario vor, in dem sich Web Gateway zwischen den Endpunkten in Ihrem Netzwerk und dem Internet befindet. Diese Web Gateway-Appliance ist in ein Advanced Threat Defense-Cluster integriert, das aus drei Advanced Threat Defense Appliances besteht.

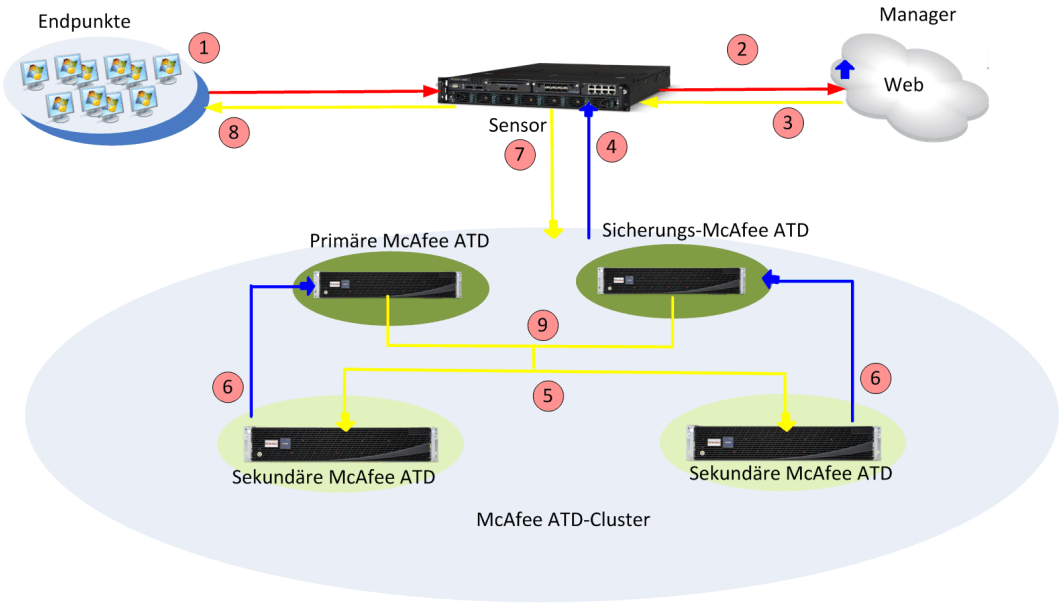


Abbildung 8-4 Web Gateway integriert in ein Advanced Threat Defense-Cluster

Nummer	Beschreibung
1	Die Endpunkte versuchen, Web-Objekte herunterzuladen.
2	Web Gateway leitet diese Anfragen weiter.
3	Wenn eine Datei heruntergeladen wird, scannt die native McAfee Gateway Anti-Malware Engine auf Web Gateway die Datei und ermittelt den Malware-Faktor.
4	Auf Grundlage des Dateityps und des Malware-Faktors ermittelt Web Gateway, ob die Datei zur Analyse an Advanced Threat Defense gesendet werden muss, und leitet die Datei, falls erforderlich, an den Verwaltungsport der primären Advanced Threat Defense weiter.
5	Die primäre Advanced Threat Defense verteilt solche Dateien unter den Mitgliedern nach dem Round-Robin-Verfahren. Sämtliche Kommunikation zwischen den Mitgliedern in einem Cluster erfolgt über deren Verwaltungsports. Angenommen, die Datei wird an eine sekundäre Advanced Threat Defense zur Analyse gesendet. Die sekundäre Advanced Threat Defense gibt die Auftrags-ID und die Task-ID an den primären Knoten zurück und beginnt mit der Analyse der Datei. Der primäre Knoten wiederum gibt die Auftrags-ID und die Task-ID an Web Gateway zurück.

Nummer	Beschreibung
6	Für die Analyseberichte stellt Web Gateway eine Anfrage an den primären Knoten mit der Task-ID. Anhand der Task-ID erkennt der primäre Knoten die Advanced Threat Defense, die die Datei analysiert hat, und ruft aus dieser die Berichte ab.
7	Als Antwort auf die Anfrage von Web Gateway leitet die primäre Advanced Threat Defense die Berichte weiter.
8	Auf Grundlage des Berichts von Advanced Threat Defense lässt Web Gateway die Datei zu oder blockiert sie.
9	Die Sicherungs-Advanced Threat Defense übernimmt die Rolle der primären Advanced Threat Defense, wenn die eigentliche primäre Advanced Threat Defense ausfällt.

Hinweise:

- Wenn Web Gateway eine Anfrage nach einem MD5-Hashwert mit Zeitraum stellt (ohne Auftrags- oder Task-ID), prüft der primäre Knoten den MD5-Hash in seiner Datenbank. Sollte es keinen passenden Eintrag geben, prüft der primäre Knoten die sekundären Knoten, wo die Datei analysiert wird, und sendet den Bericht zurück an Web Gateway, ohne die entsprechende Datei erneut zu analysieren.
- Wenn Web Gateway eine Anfrage nach einem MD5-Hashwert für einen laufenden Task stellt (ohne Auftrags- oder Task-ID), prüft der primäre Knoten den MD5-Hash mit Status (Warten oder Analysieren) in seiner Datenbank. Sollte es keinen passenden Eintrag geben, prüft der primäre Knoten die sekundären Knoten, wo die Datei analysiert wird oder in der Warteschlange ist. Dann sendet der primäre Knoten die Details zum Task an Web Gateway zurück, ohne die entsprechende Datei erneut zu analysieren.

Konfigurieren eines Advanced Threat Defense-Clusters – Grundlegende Schritte

Mit diesen grundlegenden Schritten können Sie ein Advanced Threat Defense-Cluster konfigurieren.

1. Legen Sie die Advanced Threat Defense Appliances fest, die Sie zur Erstellung des Clusters verwenden möchten. Sie können einem bereits bestehenden Advanced Threat Defense-Cluster zusätzliche sekundäre Knoten hinzufügen.
2. Stellen Sie sicher, dass die Advanced Threat Defense Appliances die unterVoraussetzungen und Anmerkungen auf Seite 322 aufgeführten Anforderungen erfüllen.
3. Legen Sie diejenige der Advanced Threat Defense Appliances fest, die als primärer Knoten dienen soll. Alle anderen Advanced Threat Defense Appliances werden als sekundäre Knoten eingestuft. Nach der Definition des Clusters können Sie den primären Knoten nur noch ändern, wenn Sie das gesamte Cluster neu definieren. Auch der Sicherungsknoten kann nach dessen Hinzufügung nicht mehr geändert werden, außer er wird aus dem Cluster entfernt.

   Bedenken Sie bei der Festlegung des primären Knotens Folgendes:

   - Verwenden Sie zum Senden von Dateien und Verwalten der Konfiguration die IP-Adresse des primären Knotens.
   - Produkte wie Network Security Platform, Web Gateway und Email Gateway müssen mit der IP-Adresse des primären Knotens integriert werden. Da Ergebnisse und Berichte über den primären Knoten abgerufen werden, ist eine Verbindung zwischen den integrierten Produkten und den sekundären Knoten nicht obligatorisch. Ab Version 3.4.2 ist die Cluster-IP der Verbindungspunkt für die integrierten Produkte, wenn der Benutzer sich für die Konfiguration eines Sicherungsknotens entscheidet.

- Stellen Sie sicher, dass die Analyse-VMs und die VM-Profile in allen Knoten identisch sind.

  Wenn Sie eine Analyse-VM hinzufügen oder ein VM-Profil hinzufügen, ändern oder löschen müssen, lösen Sie das Cluster auf, nehmen Sie in allen Knoten die erforderlichen Änderungen vor, und erstellen Sie das Cluster erneut.

- Die synchronisierten Konfigurationen der sekundären Knoten werden mit der Konfiguration des primären Knotens überschrieben. Verwenden Sie nach der Erstellung des Clusters den primären Knoten, um die Konfigurationen zu verwalten. Weitere Informationen zu synchronisierten Konfigurationen finden Sie unter Funktionsweise des Advanced Threat Defense-Clusters auf Seite 325.

4 Stellen Sie sicher, dass die sekundären Knoten und der primäre Knoten über die Verwaltungsports miteinander kommunizieren können.

5 Es wird empfohlen, vor der Konfiguration des Clusters eine Sicherung aller Knoten, insbesondere der sekundären Knoten, zu erstellen.

6 Vergewissern Sie sich, dass die integrierten Produkte so konfiguriert sind, dass sie den primären Knoten verwenden. Dies gilt auch für die integrierten Produkte von McAfee sowie für Drittanbieteranwendungen und -skripte, die die Advanced Threat Defense-REST-APIs verwenden. Ab Version 3.4.2 ist die Cluster-IP der Verbindungspunkt für die integrierten Produkte, wenn der Benutzer sich für die Konfiguration eines Sicherungsknotens entscheidet.

7 Erstellen des McAfee Advanced Threat Defense-Clusters auf Seite 332.

8 Senden Sie Dateien und URLs an das Advanced Threat Defense-Cluster.

9 Zeigen Sie die Analyseergebnisse für ein Advanced Threat Defense-Cluster an.

10 Verwalten Sie die Cluster-Konfigurationen.

Erstellen des McAfee Advanced Threat Defense-Clusters

Bevor Sie beginnen

- Sie haben den Abschnitt Konfigurieren eines Advanced Threat Defense-Clusters – Grundlegende Schritte auf Seite 331 gelesen.
- Sie besitzen Administratorrechte für die Web-Anwendung des primären Knotens.
- Die primären und sekundären Knoten sind nicht Teil eines Clusters.
- Die Softwareversion (aktive Version) aller Knoten, die Sie verwenden möchten, stimmt exakt überein.

Vorgehensweise

1 Identifizieren Sie eine Advanced Threat Defense Appliance als primären Knoten, und melden Sie sich bei dieser Web-Anwendung an.

Verwenden Sie den Namen eines Benutzers mit Administratorrechten.

2 Wählen Sie **Manage (Verwalten)** | **Load Balancing (Lastenausgleich)**.

Die Seite **Load Balancing Cluster Setting** (Einstellungen für Lastenausgleichscluster) wird angezeigt.

3 Geben Sie im Feld **Node IP address** (Knoten-IP-Adresse) die Verwaltungsport-IP-Adresse des primären Knotens ein, und wählen Sie **Primary** (Primär) aus der Dropdown-Liste aus. Klicken Sie auf **Add Node** (Knoten hinzufügen).

4 Bestätigen Sie, dass Sie das Cluster erstellen möchten.

Advanced Threat Defense legt sich selbst als primären Knoten für das Cluster fest.

5 Geben Sie im Feld **Node IP address** (Knoten-IP-Adresse) die Verwaltungsport-IP-Adresse des sekundären Knotens ein, und wählen Sie **Secondary** (Sekundär) aus. Klicken Sie auf **Add Node** (Knoten hinzufügen).

6 Klicken Sie auf**Yes** (Ja), um den sekundären Knoten hinzuzufügen.

Wenn Sie in der Bestätigungsmeldung auf **Yes** (Ja) klicken, speichert der primäre Knoten seine Konfiguration in einer Datei und sendet sie an den sekundären Knoten. Diese Datei enthält die Konfigurationen, die in diesem Dokument als synchronisierte Konfigurationen bezeichnet werden. Weitere Informationen zu synchronisierten Konfigurationen finden Sie unter Funktionsweise des Advanced Threat Defense-Clusters auf Seite 325. Der sekundäre Knoten verwendet diese Konfigurationsdatei, um die entsprechende Konfiguration in seiner Datenbank zu überschreiben. Erstellen Sie unbedingt eine Sicherung der Konfiguration für den sekundären Knoten, bevor Sie fortfahren. Wenn Sie den sekundären Knoten aus dem Cluster entfernen, wird die Konfiguration des primären Knotens beibehalten.

7 Fügen Sie die anderen sekundären Knoten auf ähnliche Weise hinzu.

8 Geben Sie im Menü **Cluster IP address** (Cluster-IP-Adresse) die Cluster-IP-Adresse ein, und klicken Sie auf **Save** (Speichern). Wählen Sie **Backup** (Sichern) aus dem Dropdown-Menü aus, und geben Sie die Verwaltungsport-IP-Adresse in das Feld **Node IP address** (Knoten-IP-Adresse) des Sicherungsknotens ein. Klicken Sie auf **Add Node** (Knoten hinzufügen), und der Sicherungsknoten wird hinzugefügt.

9 Die Details zu allen Knoten im Cluster werden in einer Tabelle angezeigt. Ähnlich wie bei anderen Tabellen in den Benutzeroberflächen der Advanced Threat Defense-Web-Anwendung können Sie die Spalten sortieren sowie die erforderlichen Spalten ausblenden oder anzeigen.

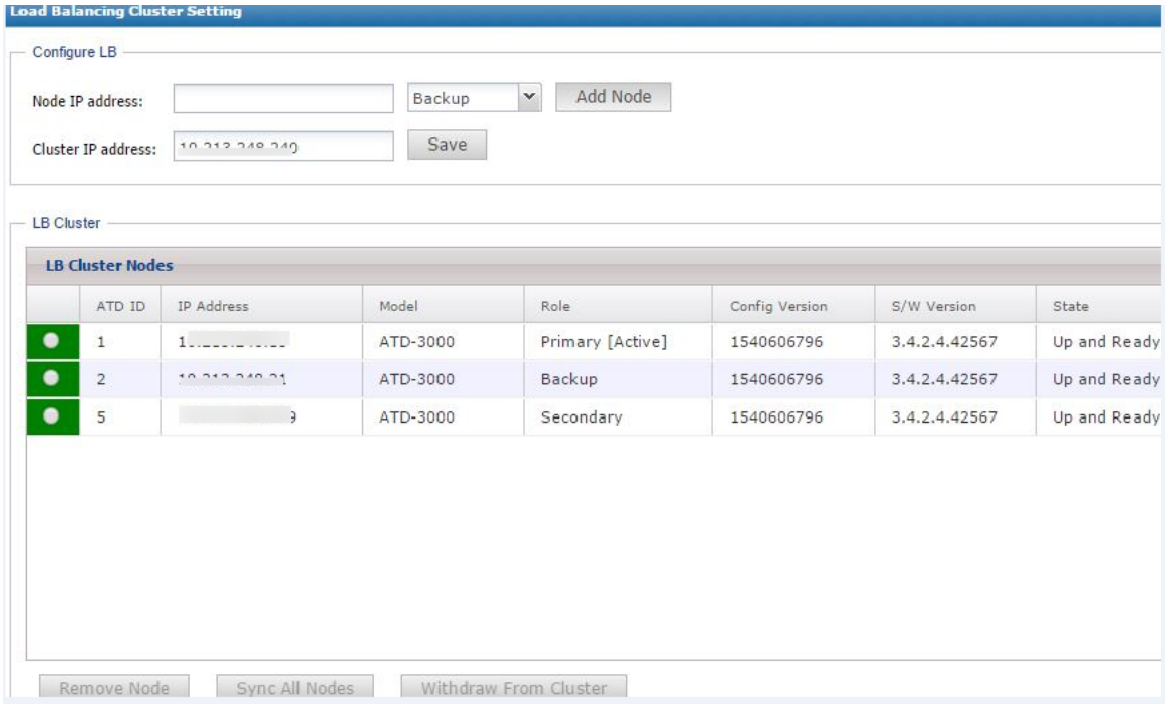


Abbildung 8-5 Erstellung eines Advanced Threat Defense-Clusters

Mit Ausnahme von **ATD ID** (ATD-ID), **IP Address** (IP-Adresse), **Role** (Rolle) und **Withdraw From Cluster** (Aus Cluster entfernen) ist keine der Optionen auf der Seite **Load Balancing Cluster Setting** (Einstellungen für Lastenausgleichscluster) für sekundäre Knoten verfügbar.

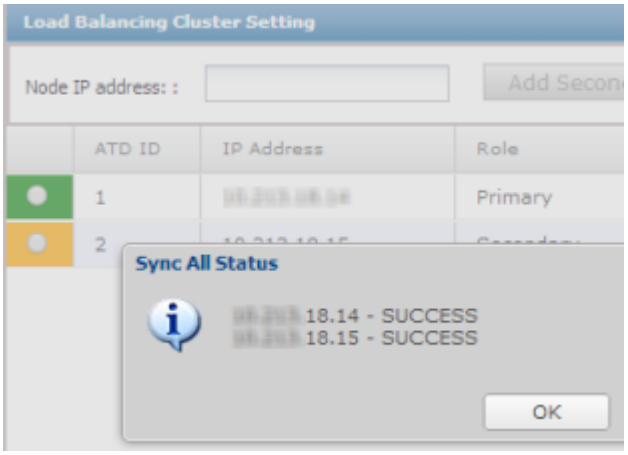
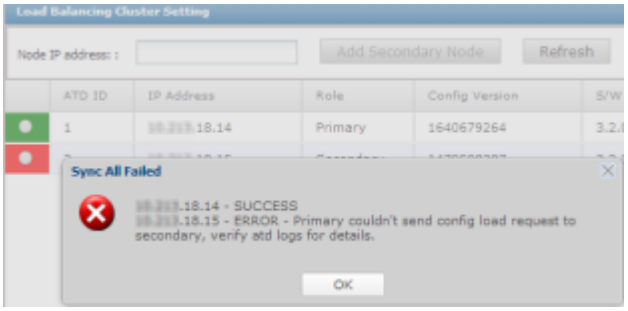
Tabelle 8-1 Optionsbeschreibungen

Option	Beschreibung
Node IP address (Knoten-IP-Adresse)	Geben Sie die Verwaltungsport-IP-Adresse der Advanced Threat Defense Appliance ein, die Sie dem Cluster hinzufügen möchten.
Dropdown-Liste	Wählen Sie je nach Anforderung "Primary", "Backup" oder "Secondary" ("Primär", "Sicherung" oder "Sekundär") aus.
Add Node (Knoten hinzufügen)	Klicken Sie auf diese Option, um dem Cluster den primären, sekundären und Sicherungsknoten hinzuzufügen. Die IP-Adresse des primären oder sekundären Knotens ist die IP-Adresse, mit der Sie auf die Advanced Threat Defense-Web-Anwendung zugreifen.
Cluster IP address (Cluster-IP-Adresse)	Geben Sie die Cluster-IP-Adresse ein, die vom aktiven Knoten (primären Knoten oder Sicherungsknoten) verwendet werden soll.
Save (Speichern)	Klicken Sie auf diese Schaltfläche, um die Cluster-IP zu speichern, bevor Sie einen Sicherungsknoten hinzufügen.
	Zeigt den Status eines Knotens an. •  : Gibt an, dass der Knoten hochgefahren und bereit ist. Handelt es sich um einen sekundären Knoten, bedeutet es außerdem, dass der primäre Knoten das Heartbeat-Signal des sekundären Knotens empfängt. •  : Gibt an, dass der Knoten hochgefahren ist, aber Ihre Aufmerksamkeit erfordert. Die Konfiguration ist z. B. möglicherweise nicht mit der Konfiguration des primären Knotens synchronisiert. •  : Gibt an, dass der primäre Knoten das Heartbeat-Signal des sekundären Knotens empfängt. Der primäre Knoten verteilt Dateien nur an Knoten, die den grünen Status aufweisen. Wechselt der Status eines sekundären Knotens während einer Dateiübertragung zu Gelb oder Rot, weist der primäre Knoten die Datei dem nächsten Knoten in der Warteschlange zu.
ATD ID (ATD-ID)	Dies ist ein systemgenerierter Ganzzahlwert zur Identifizierung der Knoten in einem Cluster. Der primäre Knoten generiert diesen eindeutigen Wert und weist ihn den Knoten im Cluster zu. Diese ID wird in der Verzeichnisstruktur links unter "Analysis Status" (Analysestatus) und "Analysis Results" (Analyseergebnisse) auf dem primären Knoten angezeigt. Hiermit können Sie den Knoten identifizieren, der eine bestimmte Probe analysiert hat. Die Eindeutigkeit der ATD-ID basiert auf der IP-Adresse eines Knotens, wie sie in der Datenbank des primären Knotens gespeichert ist. Beachten Sie, dass drei Knoten im Cluster vorhanden sind. Entfernen Sie den sekundären Knoten mit ATD-ID 2 aus dem Cluster, und fügen Sie ihn erneut dem Cluster hinzu. Anschließend wird dieser sekundäre Knoten derselben ATD-ID 2 zugewiesen, wenn die folgenden Bedingungen erfüllt sind: • Sie haben die IP-Adresse der ETH-0-Schnittstelle des Knotens (Verwaltungsanschluss) nicht geändert. • Die Datenbank des primären Knotens hat weiterhin einen Datensatz für die IP-Adresse des sekundären Knotens.
IP-Adresse	Die IP-Adresse des Verwaltungsports des Knotens.

Tabelle 8-1 Optionsbeschreibungen *(Fortsetzung)*

Option	Beschreibung
Modell	Der Modelltyp der Advanced Threat Defense Appliance. Er kann "ATD – 3000" oder "ATD – 600" lauten.
Rolle	Gibt an, ob ein Knoten ein primärer, ein sekundärer oder ein Sicherungsknoten ist.
Config Version (Config-Version)	Sobald Sie die synchronisierte Konfiguration speichern, sendet der primäre Knoten seine Konfigurationsdatei an die sekundären Knoten und erstellt eine Version dieser Konfigurationsdatei als Referenz. Für jeden Knoten wird die Versionsnummer der neuesten Konfigurationsdatei angezeigt. Wenn die Versionsnummer eines sekundären Knotens nicht der des primären Knotens entspricht, wird ein möglicher Unterschied zur Konfiguration des sekundären Knotens angezeigt. Die Statusfarbe für diesen sekundären Knoten wechselt damit zu Gelb. Die Ursache wird außerdem in der Spalte **Status** genannt. Der primäre Knoten überträgt seine Konfigurationsdatei mithilfe von Push automatisch an diesen Knoten. Dadurch wird sichergestellt, dass alle Knoten eine ähnliche synchronisierte Konfiguration aufweisen.
S/W Version (Softwareversion)	Gibt die Advanced Threat Defense-Softwareversion der Knoten an. Die vollständige Softwareversion muss für alle Knoten exakt übereinstimmen. Ist dies nicht der Fall, wechselt der Status für die entsprechenden Knoten zu Gelb.
Status	Gibt den Status von Knoten und alle wichtigen Informationen zu diesem Knoten an. Folgende Status sind z. B. möglich: • Up and Ready (Hochgefahren und bereit) • Heartbeat not received. (Kein Heartbeat empfangen.) • Node is on different config version. (Knoten besitzt eine andere Config-Version.)
Remove Node (Knoten entfernen)	Wählen Sie einen Knoten aus, und klicken Sie, um den Knoten aus dem Cluster zu entfernen. Die Konfiguration des primären Knotens wird beibehalten, selbst wenn Sie einen sekundären Knoten aus dem Cluster entfernen. Sie können einen primären Knoten erst entfernen, wenn alle sekundären Knoten entfernt wurden. Diese Option ist für sekundäre Knoten nicht verfügbar.

Tabelle 8-1 Optionsbeschreibungen *(Fortsetzung)*

Option	Beschreibung
Sync All Nodes (Alle Knoten synchronisieren)	Klicken Sie auf **Sync All** (Alle synchronisieren), um die Konfigurationssynchronisation für alle sekundären Knoten im Cluster auszulösen. Wenn Sie einen sekundären Knoten hinzufügen oder eine der synchronisierten Konfigurationen im primären Knoten speichern, löst der primäre Knoten automatisch eine Synchronisierung mit allen sekundären Knoten mit dem Status "Grün" und "Gelb" aus. Details der Konfigurationssynchronisation werden für jeden Knoten basierend auf dem Ergebnis der Synchronisierung (erfolgreich oder fehlgeschlagen) angezeigt.  **Abbildung 8-6 Konfigurationssynchronisation erfolgreich**  **Abbildung 8-7 Fehler bei der Konfigurationssynchronisation**
Withdraw from Cluster (Aus Cluster entfernen)	Diese Schaltfläche ist nur für sekundäre Knoten relevant. Klicken Sie, um einen sekundären Knoten aus dem Cluster zu entfernen und den sekundären Knoten als eigenständige Advanced Threat Defense Appliance zu verwenden. Beachten Sie Folgendes: Wenn der primäre Knoten ausfällt, fällt das Lastenausgleichscluster aus. Wenn der primäre Knoten ausfällt, klicken Sie in den sekundären Knoten auf **Withdraw from Cluster** (Aus Cluster entfernen), um sie aus dem Cluster zu entfernen und die sekundären Knoten als eigenständige Appliance zu verwenden.

Überwachen des Status eines Advanced Threat Defense-Clusters

Bevor Sie beginnen

Sie haben erfolgreich ein Lastenausgleichscluster erstellt, wie unter Erstellen des McAfee Advanced Threat Defense-Clusters auf Seite 332 beschrieben.

Sie können den Status eines Advanced Threat Defense-Clusters auf der Seite **Load Balancing Cluster Setting** (Einstellungen für Lastenausgleichscluster) oder unter Verwendung des Befehls `lbstats` überwachen. Nach dem Konfigurieren der Cluster-IP-Adresse können wir uns mit der Cluster-IP-Adresse anmelden, um auf die Advanced Threat Defense-Benutzeroberfläche zuzugreifen.

Vorgehensweise

1 Melden Sie sich über die Befehlszeilenschnittstelle (CLI) des primären oder eines sekundären Knotens an.

2 Führen Sie den Befehl `lbstats` aus.

Es werden separate Abschnitte für jeden Knoten angezeigt.

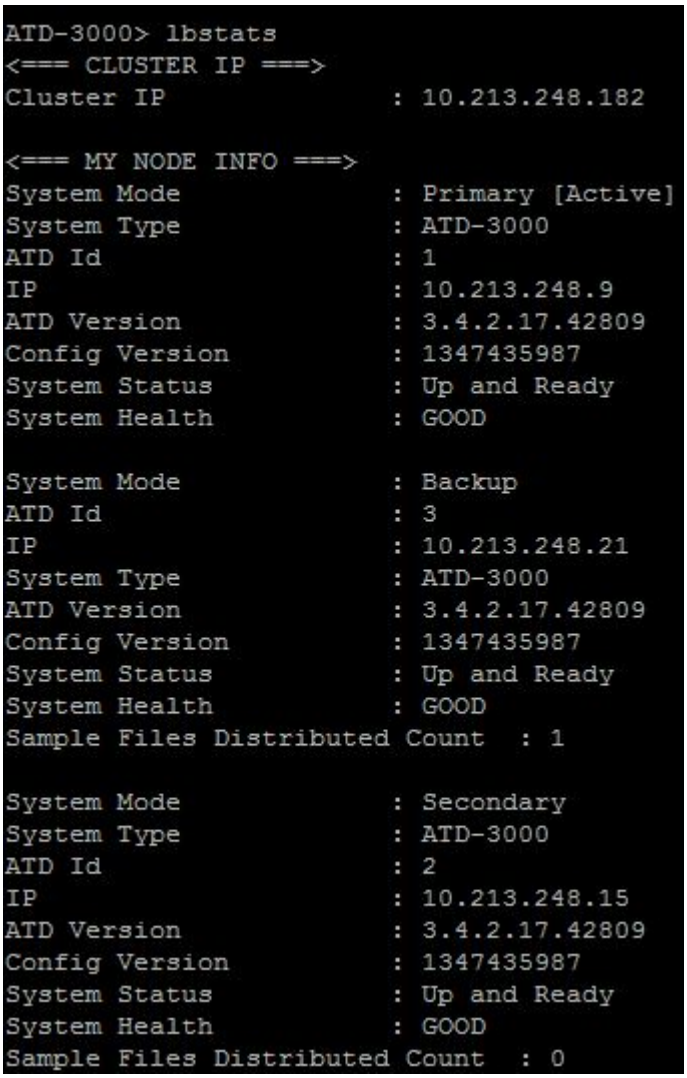

ATD-3000> lbstats
<=== CLUSTER IP ===>
Cluster IP : 10.213.248.182
<=== MY NODE INFO ===>
System Mode : Primary [Active]
System Type : ATD-3000
ATD Id : 1
IP : 10.213.248.9
ATD Version : 3.4.2.17.42809
Config Version : 1347435987
System Status : Up and Ready
System Health : GOOD
System Mode : Backup
ATD Id : 3
IP : 10.213.248.21
System Type : ATD-3000
ATD Version : 3.4.2.17.42809
Config Version : 1347435987
System Status : Up and Ready
System Health : GOOD
Sample Files Distributed Count : 1
System Mode : Secondary
System Type : ATD-3000
ATD Id : 2
IP : 10.213.248.15
ATD Version : 3.4.2.17.42809
Config Version : 1347435987
System Status : Up and Ready
System Health : GOOD
Sample Files Distributed Count : 0

Abbildung 8-8 lbstats-Ausgabe des primären Knotens

Oben ist die lbstats-Ausgabe eines primären Knotens dargestellt.

Unten ist die lbstats-Ausgabe des primären Knotens dargestellt.

```
MATDMIC1U-015> lbstats
<=== CLUSTER IP ===>
Cluster IP                : 10.213.248.182

<=== MY NODE INFO ===>
System Mode               : Secondary
System Type               : ATD-3000
ATD Id                    : 2
IP                        : 10.213.248.15
ATD Version               : 3.4.2.17.42809
Config Version            : 1347435987
System Status             : Up and Ready
System Health             : GOOD

System Mode               : Primary [Active]
ATD Id                    : 1
IP                        : 10.213.248.9

System Mode               : Backup
ATD Id                    : 3
IP                        : 10.213.248.21
```

Abbildung 8-9 lbstats-Ausgabe eines sekundären Knotens

Oben ist die lbstats-Ausgabe eines sekundären Knotens dargestellt.

```
ATD-3000> lbstats
<=== CLUSTER IP ===>
Cluster IP                : 10.213.248.182

<=== MY NODE INFO ===>
System Mode               : Backup
System Type               : ATD-3000
ATD Id                    : 3
IP                        : 10.213.248.21
ATD Version               : 3.4.2.17.42809
Config Version            : 1347435987
System Status             : Up and Ready
System Health             : GOOD

System Mode               : Primary [Active]
ATD Id                    : 1
IP                        : 10.213.248.9
System Type               : ATD-3000
ATD Version               : 3.4.2.17.42809
Config Version            : 1347435987
System Status             : Up and Ready
System Health             : GOOD

System Mode               : Secondary
System Type               : ATD-3000
ATD Id                    : 2
IP                        : 10.213.248.15
ATD Version               : 3.4.2.17.42809
Config Version            : 1347435987
System Status             : Up and Ready
System Health             : GOOD
```

Abbildung 8-10 lbstats-Ausgabe eines Sicherungsknotens

Oben ist die lbstats-Ausgabe eines Sicherungsknotens dargestellt.

Tabelle 8-2 Details zum lbstat-Befehl

Ausgabeeintrag	Beschreibung
System Mode (Systemmodus)	Gibt an, ob die Advanced Threat Defense Appliance der primäre oder ein sekundärer Knoten ist.
ATD ID (ATD-ID)	Die dem Knoten zugewiesene eindeutige ID.
IP	Die Verwaltungsport-IP-Adresse der Advanced Threat Defense Appliance.
ATD Version (ATD-Version)	Die aktuell auf dem Knoten installierte Softwareversion von Advanced Threat Defense.
Config Version (Config-Version)	Die aktuell auf dem Knoten vorhandene Version der Konfigurationsdatei.
System Status (Systemstatus)	Gibt an, ob der Knoten hochgefahren und bereit ist.

Tabelle 8-2 Details zum lbstat-Befehl *(Fortsetzung)*

Ausgabeeintrag	Beschreibung
System Health (Systemzustand)	Gibt an, ob der Knoten sich in einem gutem oder in einem nicht initialisierten Zustand befindet.
Sample Files Distributed Count (Anzahl der verteilten Probedateien)	Die Gesamtzahl der unter den Knoten, einschließlich des primären Knotens, verteilten Proben. Dieser Knoten umfasst Dateien und URLs. Diese Daten werden nur angezeigt, wenn Sie `lbstats` auf dem primären Knoten ausführen.

Einsenden von Proben an ein Advanced Threat Defense-Cluster

Zum Einsenden von Proben an ein Advanced Threat Defense-Cluster verwenden Sie den primären Knoten. Der Prozess ähnelt der Verwendung einer einzelnen Advanced Threat Defense Appliance.

- Stellen Sie sicher, dass die integrierten Produkte über Schnittstellen zum primären Knoten verfügen. Wenn Sie die Integration konfigurieren, müssen Sie die Kennwörter verwenden, die im primären Knoten konfiguriert sind. Nutzen Sie z. B. für Web Gateway den *mwg*-Benutzernamen und das im primären Knoten konfigurierte Kennwort. Ist ein Sicherungsknoten konfiguriert, dann sollte die Cluster-IP-Adresse der Kontakt für diese integrierten Produkte sein.
- Melden Sie sich zum manuellen Einsenden von Dateien und URLs mit Administratorrechten beim primären Knoten an, und senden Sie die Dateien auf dieselbe Weise ein wie bei einer eigenständigen Advanced Threat Defense Appliance. Eine Schritt-für-Schritt-Anleitung finden Sie unter Hochladen von Dateien zur Analyse mittels McAfee Advanced Threat Defense-Web-Anwendung auf Seite 280.
- Sie können auch die REST-APIs des primären Knotens verwenden, um Dateien und URLs einzusenden. Informationen dazu finden Sie im Referenzhandbuch zu McAfee Advanced Threat Defense-APIs.
- Sie können Dateien auch über FTP oder SFTP an den primären Knoten senden. Siehe Hochladen von Dateien zur Analyse über SFTP auf Seite 286



Wenn eine Cluster-IP-Adresse konfiguriert ist, müssen Sie sich anmelden und die Dateien unter Verwendung der Cluster-IP senden.

Überwachen des Analysestatus für ein Advanced Threat Defense-Cluster

Auf der Seite **Analysis Status** (Analysestatus) des primären Knotens wird der Analysestatus für Dateien, die von jedem Knoten analysiert werden, angezeigt. In einem sekundären Knoten werden nur die Dateien angezeigt, die von diesem sekundären Knoten analysiert wurden.

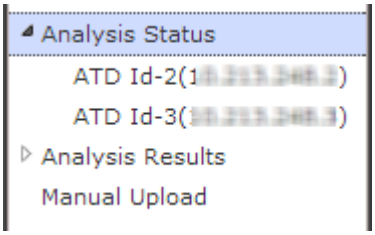
Ähnlich wie bei einer eigenständigen Advanced Threat Defense können Sie den Status der von Ihnen gesendeten Proben anzeigen. Wenn Sie Administratorrechte haben, können Sie den Status für Proben anzeigen, die von einem beliebigen Benutzer gesendet wurden.

Vorgehensweise

1 Melden Sie sich bei der Web-Anwendung des primären Knotens an.

2 Wählen Sie **Analyse** | **Analysis Status (Analysestatus)** aus.

Analysis Status (Analysestatus) kann erweitert werden, damit die sekundären Knoten des Clusters angezeigt werden. **Analysis Status** (Analysestatus) bezieht sich auf den primären Knoten. Die sekundären Knoten werden unter **Analysis Status** (Analysestatus) mit ihrer ATD-ID und ihrer Verwaltungsport-IP-Adresse aufgelistet.



3 Um den Status der durch den primären Knoten analysierten Dateien anzuzeigen, klicken Sie auf **Analysis Status** (Analysestatus).

4 Um den Status der durch einen bestimmten sekundären Knoten analysierten Dateien anzuzeigen, klicken Sie auf die entsprechende ATD-ID.

Details zu den Optionen auf der Seite **Analysis Status** (Analysestatus) finden Sie unter Konfigurieren der Seite "Analysis Status" (Analysestatus) auf Seite 290.

Überwachen von Analyseergebnissen für ein Advanced Threat Defense-Cluster

Auf der Seite **Analysis Results** (Analyseergebnisse) des primären Knotens werden die Analyseergebnisse für Dateien, die von jedem Knoten analysiert werden, angezeigt. In einem sekundären Knoten werden nur die Dateien angezeigt, die von diesem sekundären Knoten analysiert wurden.

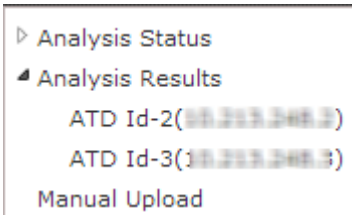
Ähnlich wie bei einer eigenständigen Advanced Threat Defense können Sie die Ergebnisse der von Ihnen gesendeten Proben anzeigen. Wenn Sie Administratorrechte haben, können Sie die Ergebnisse für Proben anzeigen, die von einem beliebigen Benutzer gesendet wurden.

Vorgehensweise

1 Melden Sie sich als *admin*-Benutzer bei einem der Knoten des Advanced Threat Defense-Clusters an.

2 Wählen Sie **Analyse** | **Analysis Results (Analyseergebnisse)** aus.

Analysis Results (Analyseergebnisse) kann erweitert werden, damit die sekundären Knoten des Clusters angezeigt werden. **Analysis Results** (Analyseergebnisse) bezieht sich auf den primären Knoten. Die sekundären Knoten werden unter **Analysis Results** (Analyseergebnisse) mit ihrer ATD-ID und ihrer Verwaltungsport-IP-Adresse aufgelistet.



3 Um die Ergebnisse der durch den primären Knoten analysierten Dateien anzuzeigen, klicken Sie auf **Analysis Results** (Analyseergebnisse).

4 Um die Ergebnisse der durch einen bestimmten sekundären Knoten analysierten Dateien anzuzeigen, klicken Sie auf die entsprechende ATD-ID.

Details zu den Optionen auf der Seite **Analysis Results** (Analyseergebnisse) finden Sie unter Anzeigen der Analyseergebnisse auf Seite 294.

Ändern der Konfigurationen für einMcAfee Advanced Threat Defense-Cluster

In Bezug auf ein McAfee Advanced Threat Defense-Cluster können Konfigurationen in zwei Typen klassifiziert werden:

- Einstellungen, die nur über den primären Knoten konfiguriert werden. Zu Erklärungszwecken werden diese Einstellungen in diesem Dokument als *synchronisierte Konfiguration* bezeichnet.
- Einstellungen, die in jedem Knoten eines McAfee Advanced Threat Defense-Clusters individuell konfiguriert werden. Diese Einstellungen werden als *nicht synchronisierte Konfiguration* bezeichnet.

Synchronisierte Konfiguration – Die folgenden Einstellungen fallen in diese Kategorie:

- Verwalten von Analyseprofilen auf Seite 251
- Verwalten von McAfee Advanced Threat Defense-Benutzern auf Seite 37
- Integration in McAfee ePO auf Seite 256
- Konfigurieren des Proxy-Servers für die Internetverbindung auf Seite 261
- Konfigurieren von DNS-Einstellungen auf Seite 267
- Konfigurieren der Datums- und Uhrzeiteinstellungen auf Seite 267

Melden Sie sich mit Administratorrechten beim primären Knoten an, um die oben aufgelisteten Einstellungen zu konfigurieren. Wenn Sie auf den entsprechenden Seiten auf **Save** (Speichern) klicken, bündelt der primäre Knoten die gesamte *synchronisierte Konfiguration* in einer Datei und sendet sie an alle verfügbaren sekundären Knoten. Die sekundären Knoten speichern diese Einstellungen in ihrer Datenbank und verwenden sie später. Dieser Konfigurationsdatei wird eine Versionsnummer zugewiesen. Die Versionsnummer ist die **Config Version** (Config-Version), die auf der Seite **Load Balancing Cluster Setting** (Einstellungen für Lastenausgleichscluster) aufgelistet ist.

Der primäre Knoten sendet die Konfigurationsdatei über einen sicheren Kommunikationskanal an die sekundären Knoten. Sie können die Spalte **State** (Status) auf der Seite **Load Balancing Cluster Setting** (Einstellungen für Lastenausgleichscluster) überprüfen, um sicherzugehen, dass die Konfigurationsdatei erfolgreich auf einen sekundären Knoten angewendet wurde. Alternativ können Sie für den primären Knoten auf der Seite **Load Balancing Cluster Setting** (Einstellungen für Lastenausgleichscluster) auf **Sync All Nodes** (Alle Knoten synchronisieren) klicken, um die Konfigurationsdatei an alle verfügbaren Knoten zu senden. Sollte ein sekundärer Knoten ausgefallen sein, wird dies in der Spalte **State** (Status) angezeigt.



Wenn der primäre Knoten die Konfiguration für das Cluster synchronisiert, sendet er die gesamten *synchronisierten Daten* an alle verfügbaren Knoten im Cluster. Das bedeutet, dass Sie sekundäre Knoten nicht selektiv synchronisieren können. Sie können auch nicht die Konfigurationen auswählen, die Sie an die sekundären Knoten senden möchten. Der Prozess der Konfigurationssynchronisation hat keinerlei Auswirkungen auf die Lastenausgleichs- oder Dateianalyseprozesse einer McAfee Advanced Threat Defense Appliance.

Nicht synchronisierte Konfiguration – Die folgenden Einstellungen fallen in diese Kategorie:

- Upgrade der McAfee Advanced Threat Defense-Software von 3.0.2.xx auf 3.0.4.xx auf Seite 45
- Erstellen einer Analyse-VM auf Seite 4

- Verwalten von VM-Profilen auf Seite 233
- DAT- und Scan-Modul-Versionen der McAfee Anti-Malware Engine
- DAT- und Scan-Modul-Versionen der McAfee Gateway Anti-Malware Engine
- Whitelist- und Blacklist-Einträge
- Benutzerdefinierte YARA-Regeln
- Konfigurationen für die Datenbanksicherung und -wiederherstellung
- Alle mit der CLI vorgenommenen Konfigurationen

Melden Sie sich bei jedem Knoten im Cluster an, um diese Konfigurationen zu ändern. Stellen Sie sicher, dass die Konfigurationen in allen Knoten des Clusters identisch sind.

9

CLI-Befehle für McAfee Advanced Threat Defense

Die McAfee Advanced Threat Defense-Appliance unterstützt CLI-Befehle (Command Line Interface, Befehlszeilenschnittstelle) für Aufgaben wie Netzwerkkonfiguration, Neustarten der Appliance und Zurücksetzen der Appliance auf die Werkseinstellungen.

Inhalt

- *Ausgabe von CLI-Befehlen*
- *CLI-Syntax*
- *Anmelden über die Befehlszeilenschnittstelle (CLI)*
- *Bedeutung von "?"*
- *Verwalten der Festplatten der McAfee Advanced Threat Defense Appliance*
- *Liste der CLI-Befehle*

Ausgabe von CLI-Befehlen

Sie können CLI-Befehle lokal über die McAfee Advanced Threat Defense Appliance-Konsole oder auch per Fernzugriff mittels SSH ausgeben.

Ausgeben eines Befehls über die Konsole

Informationen zum Einrichten der Konsole für eine McAfee Advanced Threat Defense-Appliance finden Sie unterKonfigurieren der Netzwerkinformationen für die McAfee Advanced Threat Defense Appliance auf Seite 31.



Falls in der Dokumentation angegeben wird, dass Sie einen Vorgang "auf der Appliance" durchführen sollen, bedeutet das, dass Sie den Vorgang über die Befehlszeile eines Konsolenhosts durchführen, der mit der McAfee Advanced Threat Defense-Appliance verbunden ist. Beispiel: Wenn Sie die Netzwerkdetails für eine McAfee Advanced Threat Defense-Appliance zum ersten Mal konfigurieren, müssen Sie dies über die Konsole tun.

Wenn die Verbindung mit der McAfee Advanced Threat Defense-Appliance erfolgreich hergestellt wurde, sehen Sie die Anmeldeaufforderung.

Ausgeben eines Befehls über SSH

Sie können eine McAfee Advanced Threat Defense-Appliance standortfern mittels Eingabeaufforderung über `SSH` verwalten.

Es können nur 5 SSHD-CLI-Sitzungen gleichzeitig auf einer McAfee Advanced Threat Defense-Appliance aktiv sein.

Anmeldung bei der McAfee Advanced Threat Defense Appliance mittels SSH-Client

Vorgehensweise

1. Öffnen Sie eine SSH-Clientsitzung.
2. Geben Sie die IPv4-Adresse der McAfee Advanced Threat Defense Appliance und bei der Portnummer "2222" ein.
3. Geben Sie im Anmeldebildschirm den Standardbenutzernamen `cliadmin` und das Standardkennwort `atdadmin` ein.

   Die Höchstanzahl von Anmeldeversuchen bei der McAfee Advanced Threat Defense Appliance ist auf drei festgelegt. Danach wird die Verbindung beendet.

   Die Höchstanzahl der Anmeldeversuche bei der McAfee Advanced Threat Defense Appliance kann je nach verwendetem SSH-Client variieren. Bei manchen Clients (z. B. Putty Version 0.54 und 0.56) liegt sie bei drei, bei anderen (z. B. Putty Version 0.58 und Linux-SSH-Clients) beträgt sie vier.

Auto-Vervollständigung

Die Befehlszeilenschnittstelle (CLI) verfügt über eine Auto-Vervollständigungsfunktion. Drücken Sie zur Auto-Vervollständigung eines Befehls die **Tab**-Taste, nachdem Sie einige Zeichen eines gültigen Befehls eingegeben haben, und anschließend die **Enter**-Taste. Beispiel: Wenn Sie `pas` tippen und die **Tab**-Taste drücken, würde CLI die Eingabe automatisch mit dem Befehl `passwd` vervollständigen.

Gibt es für den teilweise eingegebenen Text mehrere Optionen, zeigt CLI alle verfügbaren und passenden Befehle an.

CLI-Syntax

Geben Sie bei Eingabeaufforderung Befehle wie folgt ein:

```
<command> <value>
```

- Obligatorische Werte stehen in spitzen Klammern (< >).
- Optionale Schlüsselwörter oder Werte stehen in eckigen Klammern ([ ]).
- Optionen werden durch eine Linie (|) getrennt angezeigt.
- Variablen werden *kursiv* dargestellt.

Geben Sie die Symbole "< >" oder "[ ]" nicht ein.

Obligatorische Befehle

Bestimmte Befehle müssen in der McAfee Advanced Threat Defense Appliance ausgeführt werden, bevor sie voll funktionsfähig ist. Die übrigen Befehle in diesem Kapitel sind optional und haben Standardwerte als Parameter, sofern sie nicht mit anderen spezifischen Parameterwerten ausgeführt werden.

Dies sind die erforderlichen Befehle:

- `set appliance name`
- `set appliance ip`
- `set appliance gateway` wird in folgenden Fällen ebenfalls benötigt:
  - Wenn sich die McAfee Advanced Threat Defense Appliance in einem anderen Netzwerk befindet als die McAfee-Produkte, in die Sie sie integrieren möchten
  - Wenn Sie von einem anderen Netzwerk aus auf McAfee Advanced Threat Defense zugreifen möchten, entweder über einen SSH-Client oder per Browserzugriff auf die McAfee Advanced Threat Defense-Web-Anwendung

Anmelden über die Befehlszeilenschnittstelle (CLI)

Bevor Sie CLI-Befehle eingeben können, müssen Sie sich zunächst mit einem gültigen Benutzernamen (Standard-Benutzername ist `cliadmin`) und einem Kennwort (Standard ist `atdadmin`) bei der McAfee Advanced Threat Defense Appliance anmelden. Zum Abmelden geben Sie `exit` ein.



Es wird von McAfee dringend empfohlen, das Kennwort zu ändern, indem Sie bei Ihrer ersten Interaktion mit der McAfee Advanced Threat Defense Appliance den Befehl `passwd` verwenden.

Bedeutung von "?"

`?` zeigt mögliche Befehlszeichenfolgen, die Sie eingeben können, an.

Syntax:

`?`



`?` in Kombination mit einem anderen Befehl zeigt das nächste Wort an, das Sie eingeben können. Wenn Sie beispielsweise den ?-Befehl zusammen mit dem `set`-Befehl eingeben, erhalten sie eine Liste aller Optionen für den `set`-Befehl.

Verwalten der Festplatten der McAfee Advanced Threat Defense Appliance

Die McAfee Advanced Threat Defense Appliance hat zwei Festplatten: Disk-A und Disk-B. "Disk-A" ist die aktive Festplatte, und "Disk-B" ist die Sicherungsfestplatte. Auch wenn "Disk-A" nicht gestartet wird, wird sie dennoch als die aktive Festplatte bezeichnet. Gleichfalls wird "Disk-B" als die Sicherungsfestplatte bezeichnet, auch wenn sie nicht gestartet wird. Standardmäßig enthalten beide Festplatten die vorinstallierte Softwareversion. Sie können die Software auf der aktiven Festplatte, also "Disk-A", aktualisieren und "Disk-B" verwenden, um eine Sicherungskopie einer stabilen Version zu erstellen, die Sie immer wiederherstellen können.

Verwenden Sie den Befehl `show`, um die gespeicherte Softwareversion auf der aktiven bzw. der Sicherungsfestplatte anzuzeigen.

Tabelle 9-1 CLI-Befehle zur Festplattenverwaltung

Befehl	Beschreibung
`copyto backup`	Der Befehl kopiert die Softwareversion von der aktiven Festplatte auf die Sicherungsfestplatte. Wenn beispielsweise die aktuelle aktive Softwareversion stabil ist, können Sie sie auf die Sicherungsfestplatte kopieren. Der Befehl funktioniert nur, wenn die Appliance von der aktiven Festplatte gestartet wurde.
`copyto active`	Der Befehl kopiert die Softwareversion von der Sicherungsfestplatte auf die aktive Festplatte. Sie müssen jedoch die McAfee Advanced Threat Defense Appliance neu starten, damit das neue Image von der aktiven Festplatte geladen wird. Der Befehl funktioniert nur, wenn die Appliance von der Sicherungsfestplatte gestartet wurde.
`reboot backup`	Der Befehl startet die Appliance neu, mit der Softwareversion auf der Sicherungsfestplatte.
`reboot active`	Der Befehl startet die Appliance neu, mit der Softwareversion auf der aktiven Festplatte.

Liste der CLI-Befehle

In diesem Abschnitt sind die CLI-Befehle für McAfee Advanced Threat Defense in alphabetischer Reihenfolge aufgeführt.

amas

Verwenden Sie diesen Befehl, um amas-Dienste zu starten, anzuhalten und erneut zu starten.

Syntax: `amas <word>`

Parameter	Beschreibung
<WORD>	Dies ist der amas-Dienst, den Sie anhalten möchten.

Beispiel: `amas start/stop/restart`

atdcounter

Zeigt den modulspezifischen Zähler an, z. B. durch GTI, MAV, GAM, amas usw. gesendete und verarbeitete Dateien.

Syntax: `atdcounter`

Dieser Befehl hat keine Parameter.

backup reports

Mit diesem Befehl wird eine Sicherung der McAfee Advanced Threat Defense-Berichte auf einem externen FTP-/SFTP-Server erstellt, der für einen Benutzer unter den Schnittstellenports der FTP-Ergebnisausgabe-Einstellungen konfiguriert ist.

Syntax

```
backup reports
```

Dieser Befehl hat keine Parameter.

backup reports date

Mit diesem Befehl wird eine Sicherung der McAfee Advanced Threat Defense-Berichte für einen bestimmen Zeitraum auf einem externen FTP-/SFTP-Server erstellt, der für einen Benutzer unter den Einstellungen der FTP-Ergebnisausgabe konfiguriert ist.

Syntax: `backup reports date <yyyy-mm-dd>`

Parameter	Beschreibung
yyyy-mm-dd yyyy-mm-dd	Der Zeitraum, für den eine Sicherung von Berichten erstellt werden soll.

Beispiel: `2014-07-10 2014-07-12`

Blacklist

Verwenden Sie folgende Befehle, um die McAfee Advanced Threat Defense-Blacklist zu verwalten.

Syntax:

- Verwenden Sie `blacklist add <md5> <score> <file_name> <malware_name> <Eng-ID> <OS-ID>`, um der Blacklist einen MD5-Werthinzuzufügen.

Parameter	Beschreibung
<md5>	Der MD5-Hashwert einer Malware, den Sie der Blacklist hinzufügen möchten
<score>	Der Malware-Schweregrad, gültige Werte sind 3 bis 5
<file_name>	Der Dateiname für den MD5-Wert
<malware_name>	Der Malware-Name für den MD5-Wert
<Eng-ID>	Die numerische ID für das entsprechende Modul
<OS-ID>	Die numerische ID des Betriebssystems, das für die dynamische Analyse der Malware verwendet wurde

  Beispiel: `blacklist add 254A40A56A6E28636E1465AF7C42B71F 3 ExampleFileName ExampleMalwareName 3 3`

- Verwenden Sie `blacklist delete <md5>`, um einen MD5-Wert von der Blacklist zu löschen.

Parameter	Beschreibung
<md5>	Der MD5-Hashwert einer Malware, den Sie von der Blacklist löschen möchten

  Beispiel: `blacklist delete 254A40A56A6E28636E1465AF7C42B71F`

- Verwenden Sie `blacklist query <md5>`, um zu überprüfen, ob ein MD5-Wert in der Blacklist vorhanden ist.

Parameter	Beschreibung
<md5>	Der MD5-Hashwert einer Malware, für den Sie überprüfen möchten, ob er in der Blacklist vorhanden ist

Beispiel: `blacklist query 254A40A56A6E28636E1465AF7C42B71F`

Ist der MD5-Wert vorhanden, werden Details wie die Modul-ID, der Malware-Schweregrad und so weiter angezeigt.

- Verwenden Sie `blacklist update <md5> <score> <file_name> <malware_name> <Eng-ID> <OS-ID>`, um die Details für einen Eintrag in der Blacklist zu aktualisieren.

Parameter	Beschreibung
<md5>	Der MD5-Hashwert einer Malware, den Sie aktualisieren möchten; Wert muss in der Blacklist vorhanden sein, damit Sie den Datensatz aktualisieren können
<score>	Der neue Malware-Schweregrad, den Sie ändern möchten; gültige Werte sind 3 bis 5
<file_name>	Der neue Dateiname für den MD5-Wert
<malware_name>	Der neue Malwarename für den MD5-Wert
<Eng-ID>	Die neue Modul-ID, auf die geändert werden soll
<OS-ID>	Der neue Wert des Betriebssystems, das für die dynamische Analyse der Malware verwendet wurde

Beispiel: `blacklist update 254A40A56A6E28636E1465AF7C42B71F 4 ExampleFileName ExampleMalwareName 3 4`

clearstats

Dieser Befehl setzt alle McAfee Advanced Threat Defense-Statistiken auf null zurück.

Syntax: `clearstats`

Dieser Befehl hat keine Parameter.

cluster withdraw

Mit diesem Befehl werden Cluster mithilfe von CLI gelöscht. Er kann für alle Knoten ausgeführt werden (primär/sekundär/Sicherungsknoten). Der Befehl löscht alle clusterspezifischen Konfigurationen aus diesem Knoten und richtet ihn als eigenständiges Gerät ein.

Dieser Befehl kann für Szenarien verwendet werden, in denen der Knoten mit den üblichen Entfernungsmethoden wie "Remove Node" (Knoten entfernen) oder "Withdraw from Cluster" (Aus Cluster entfernen) nicht gelöscht werden kann.

Syntax: `cluster withdraw`

Dieser Befehl hat keine Parameter.

createDefaultVms

Mit diesem Befehl erstellen Sie Standardanalyse-VMs.

Syntax: `createDefaultVms`

Dieser Befehl hat keine Parameter.

db_repair

Repariert die ATD-Datenbank, falls die Datenbank beschädigt wurde.

Syntax: `db_repair`

Dieser Befehl hat keine Parameter.

deleteblacklist

Verwenden Sie diesen Befehl, um alle Einträge aus der McAfee Advanced Threat Defense-Blacklist zu entfernen.

Syntax: `deleteblacklist`

Dieser Befehl hat keine Parameter.

deletesamplereport

Dieser Befehl löscht alle Analyseberichte für eine Datei.

Syntax: `deletesamplereport <md5>`

Parameter	Beschreibung
<md5>	Der MD5-Wert der Datei, für die Sie alle Berichte in McAfee Advanced Threat Defense löschen möchten.

Beispiel: `deletesamplereport c0850299723819570b793f6e81ce0495`

diskcleanup

Verwenden Sie diesen Befehl, um einige der älteren Analyseberichte zu löschen, wenn nur noch wenig Festplattenspeicher auf McAfee Advanced Threat Defense verfügbar ist.

Syntax: `diskcleanup`

Dieser Befehl hat keine Parameter.

dxlstatus

Verwenden Sie diesen Befehl, um den DXL-Status zu bestimmen.

Syntax: `dxlstatus`

Dieser Befehl hat keinen Parameter.

Unter Verwendung dieses Befehls werden die folgenden Informationen angezeigt:

```
<=== DXL STATUS ===>
Status : DISABLED
DXL Channel Status : DOWN
Sample Files Received Count : 0
Sample Files Published Count : 0
Sample Files Queued Count : 0
```

docfilterstatus

Mithilfe des Befehls "docfilterstatus" soll eine unnötige Belastung des Sandkastens durch MS Office 2007+ Word- und Excel-Dateien, die frei von verdächtigen Inhalten sind, verhindert werden. Mit diesem Befehl kann der heuristische Filter für MS Office 2007+ Word- und Excel-Dateien aktiviert oder deaktiviert werden. Verwenden Sie den Befehl "Anzeigen", um den aktuellen Status zu bestimmen.

Die heuristische Analyse ist standardmäßig aktiviert.

Syntax:

```
set docfilterstatus <enable>

set docfilterstatus <disable>

docfilterstatus<enable><disable>
```

Parameter	Beschreibung
enable	Setzt das Filtern der Proben auf "Aktiviert".
disable	Setzt das Filtern der Proben auf "Deaktiviert".

Syntax: `show docfilterstatus`

Dies ist eine Funktion von McAfee Advanced Threat Defense. Wenn sie aktiviert ist, führt McAfee Advanced Threat Defense eine heuristische Analyse einer MS Office 2007+ Word- oder Excel-Datei aus, die vom Network Security Sensor gesendet wurde. Das bedeutet, dass sie die Struktur der Office-Datei auf schädliche Inhalte wie einbettete, aktive Inhalte, Makros oder verdächtige Hyperlinks untersucht. Nur wenn heuristische Unregelmäßigkeiten in der Datei vorliegen, wird sie gemäß dem entsprechenden Analyseprofil für eine Malware-Analyse berücksichtigt. Wenn keine Unregelmäßigkeiten vorliegen, wird die Datei als sauber behandelt. Das bedeutet, dass ihr eine Schweregrad von Null (Information) zugewiesen wird.

In Netzwerken, in denen eine hohe Zahl von MS Office 2007+ Word- und Excel-Dateien gesendet wird, kann mithilfe des heuristischen Filters durch das Herausfiltern von Dateien, in denen keine verdächtigen Inhalte vorliegen, die Belastung für McAfee Advanced Threat Defense gesenkt werden.

Wenn die heuristische Analyse aktiviert ist, werden folgende Einstellungen verwendet:

- Die heuristische Filterung ist AKTIVIERT.

  Durch das Aktivieren der heuristischen Analyse wird der heuristische Filter ebenfalls AKTIVIERT, sodass McAfee Advanced Threat Defense die MS Office 2007+ Word- oder Excel-Dateistruktur auf Unregelmäßigkeiten untersucht. Wenn keine Unregelmäßigkeiten vorliegen, wird die Datei als sauber behandelt, und es wird keine weitere Analyse durchgeführt. Wenn heuristische Unregelmäßigkeiten vorliegen, wird die MS Office 2007+ Word- oder Excel-Datei gemäß dem entsprechenden Analyseprofil statisch und dynamisch analysiert.

Wenn die heuristische Analyse deaktiviert ist, werden folgende Einstellungen verwendet:

- Die heuristische Filterung ist DEAKTIVIERT.

  Durch das Deaktivieren der heuristischen Analyse wird der heuristische Filter ebenfalls DEAKTIVIERT, sodass McAfee Advanced Threat Defense die MS Office 2007+ Word- oder Excel-Dateien nicht auf heuristische Unregelmäßigkeiten untersucht. Die MS Office 2007+ Word- und Excel-Dateien werden gemäß dem entsprechenden Analyseprofil statisch und dynamisch analysiert.

exit

Der Befehl beendet die CLI.

Dieser Befehl hat keine Parameter.

Syntax:

```
exit
```

factorydefaults

Löscht alle Proben, Ergebnisse, Protokolle und Analyse-VM-Laufwerksdateien, und setzt alle IP-Adressen vor dem Neustart des Geräts zurück. Der Befehl erscheint nicht, wenn Sie `?` tippen. Auch die Auto-Vervollständigungsfunktion gilt für diesen Befehl nicht. Für die Ausführung muss er vollständig eingegeben werden.

Dieser Befehl hat keine Parameter.

- Sie erhalten eine Warnung, dass durch den Vorgang die Einstellungen der McAfee Advanced Threat Defense Appliance gelöscht werden. Sie müssen diese Aktion bestätigen. Der Grund für die Warnung ist, dass die McAfee Advanced Threat Defense Appliance auf ihren sauberen, unkonfigurierten Zustand zurückgesetzt wird, wodurch alle derzeitigen Konfigurationseinstellungen sowohl auf der aktiven als auch auf der Sicherungsfestplatte verloren gehen. Nachdem Sie den Vorgang bestätigt haben, löscht dieser Befehl sowohl auf der aktiven als auch auf der Sicherungsfestplatte sofort alle Ihre Konfigurationseinstellungen, einschließlich Proben, Ergebnisse, Protokolle und Analyse-VM-Laufwerksdateien.
- Die aktuelle Softwareversion auf der Sicherungsfestplatte wird auf der aktiven Festplatte angewendet.

Syntax:

```
factorydefaults
```

ftptest USER_NAME

Verwenden Sie diesen Befehl, um die unter "Verwalten > Benutzerverwaltung > FTP Results" (FTP-Ergebnisse) für einen bestimmten Benutzer gespeicherten FTP-Einstellungen zu testen.

Syntax: `ftptest USER_NAME`

Parameter	Beschreibung
USER_NAME	Der Benutzername, für den Sie die FTP-Einstellungen testen möchten.

Beispiel: `NSPuser`

gti-restart

Dieser Befehl startet das McAfee GTI-Modul von McAfee Advanced Threat Defense neu.

Syntax: `gti-restart`

Dieser Befehl hat keine Parameter.

help

Dieser Befehl stellt eine Beschreibung des interaktiven Hilfesystems bereit.

Dieser Befehl hat keine Parameter.

Syntax:

```
help
```

heuristic_analysis

Stellen Sie sich vor, ein Network Security Sensor sendet eine sehr große Anzahl von Dateien. Sie möchten, dass McAfee Advanced Threat Defense diese Dateien für eine detaillierte Malware-Analyse sichtet. Der Zweck dieser Sichtung besteht in einer Leistungssteigerung ohne Einbußen bei der Sicherheit. Mithilfe des Befehls "heuristic_analysis" können Sie dies erreichen.

- Aktivieren Sie den heuristischen Filter für PDF-Dateien.
- Geben Sie die Mindestdateigröße für die PDF-Dateien an, die bei der Malware-Analyse berücksichtigt werden sollen.
- Deaktivieren Sie die Option "Re-Analyze" (Erneut analysieren) für alle unterstützten Dateitypen.

Verwenden Sie den Befehl `Anzeigen`, um den aktuellen Status zu bestimmen. Die heuristische Analyse ist standardmäßig deaktiviert.

Syntax: `show heuristic_analysis`

Wenn die heuristische Analyse deaktiviert ist, werden folgende Einstellungen verwendet:

Einstellung	Beschreibung
`Die heuristische Filterung ist DEAKTIVIERT`	Dies ist eine Funktion von McAfee Advanced Threat Defense. Wenn sie aktiviert ist, führt McAfee Advanced Threat Defense eine heuristische Analyse für eine PDF-Datei aus, die vom Network Security Sensor gesendet wurde. Das bedeutet, dass sie die Struktur der PDF-Datei auf schädliche Inhalte wie einbettete Javaskripte, EXE-Dateien oder jegliche Umleitungen untersucht. Nur wenn heuristische Unregelmäßigkeiten in der Datei vorliegen, wird sie gemäß dem entsprechenden Analyseprofil für eine Malware-Analyse berücksichtigt. Wenn keine Unregelmäßigkeiten vorliegen, wird die Datei als sauber behandelt. Das bedeutet, dass ihr eine Schweregrad von Null (Information) zugewiesen wird. In Netzwerken, in denen eine hohe Zahl von PDF-Dateien gesendet wird, kann mithilfe des heuristischen Filters durch das Herausfiltern von Dateien, in denen keine verdächtigen Inhalte vorliegen, die Belastung für McAfee Advanced Threat Defense gesenkt werden.
`Konfigurationseinstellung: Re-Analyze (Erneut analysieren): AKTIVIERT`	Standardmäßig analysiert McAfee Advanced Threat Defense alle unterstützten Dateien, die von einem Sensor gesendet wurden, selbst wenn sie bereits analysiert wurden. Wenn "Re-Analyze" (Erneut analysieren) DEAKTIVIERT ist, überprüft McAfee Advanced Threat Defense anhand des MD5-Hashwerts einer Datei, ob für sie bereits Analyseergebnisse vorliegen. Wenn ja, stellt sie dem Network Security Manager die verfügbaren Ergebnisse bereit, anstatt die Datei erneut zu analysieren. Dasselbe Ergebnis wird auch in McAfee Advanced Threat Defense angezeigt.
`Konfigurationseinstellung: min file size: 2048 (Mindestdateigröße)`	Sie können für von Sensoren gesendete PDF-Dateien eine Mindestdateigröße angeben. Kleinere Dateien werden dann nicht von McAfee Advanced Threat Defense analysiert. Durch das Herausfiltern kleinerer PDF-Dateien wird die Belastung für McAfee Advanced Threat Defense gesenkt. Die Standard-Dateigröße beträgt für von Sensoren gesendete PDF-Dateien 2 KB.

Die Funktion "Re-Analyze" (Erneut analysieren) wird auf alle von Sensoren unterstützten Dateitypen angewendet, während der heuristische Filter und die Mindestdateigröße nur für von Sensoren gesendete PDF-Dateien gelten.

Verwenden Sie den Befehl `Festlegen`, um die heuristische Analyse für von einem Sensor gesendete Dateien zu aktivieren oder zu deaktivieren.

Syntax: `set heuristic_analysis <enable> <PDF minimum file size in bytes>`

Syntax: `set heuristic_analysis <disable>`

Der Befehl `set heuristic_analysis` wird nicht ausgeführt, wenn gerade eine Analyse-VM erstellt wird.

Beispiel ohne Mindestdateigröße: `set heuristic_analysis enable`

Wenn Sie dieses Beispiel ausführen, werden die folgenden Einstellungen in dieser Reihenfolge auf von einem Sensor gesendete PDF-Dateien angewendet:

1. Da Sie keine Mindestdateigröße angegeben haben, wird sie auf 2 KB festgelegt. Daher werden von McAfee Advanced Threat Defense nur PDF-Dateien mit einer Größe von mindestens 2 KB für eine weitere Analyse berücksichtigt.
2. Durch die Aktivierung der heuristischen Analyse wird "Re-Analyze" (Erneut analysieren) DEAKTIVIERT. Daher überprüft McAfee Advanced Threat Defense, ob bereits ein Analyseergebnis vorliegt. Wenn ja, wird dieses Ergebnis ohne weitere Analyse an den Manager weitergeleitet. Ist das Ergebnis nicht für denselben MD5-Hashwert verfügbar, folgt der nächste Analyseschritt.
3. Durch das Aktivieren der heuristischen Analyse wird der heuristische Filter ebenfalls AKTIVIERT, sodass McAfee Advanced Threat Defense die PDF-Dateistruktur auf Unregelmäßigkeiten untersucht. Wenn keine Unregelmäßigkeiten vorliegen, wird die Datei als sauber behandelt, und es wird keine weitere Analyse durchgeführt. Wenn heuristische Unregelmäßigkeiten vorliegen, wird die PDF-Datei gemäß dem entsprechenden Analyseprofil statisch und dynamisch analysiert.

Für Dateien, die nicht im PDF-Format vorliegen, wird nur die Option "Re-Analyze" (Erneut analysieren; siehe Schritt 2 oben) berücksichtigt.

Beispiel mit Mindestdateigröße: `set heuristic_analysis enable 5000`

Wenn Sie dieses Beispiel ausführen, werden die folgenden Einstellungen in dieser Reihenfolge auf von einem Sensor gesendete PDF-Dateien angewendet:

1. Die Mindestdateigröße wird auf 5.000 Byte festgelegt. Daher werden von der McAfee Advanced Threat Defense nur PDF-Dateien mit einer Größe von mindestens 5.000 Byte für eine weitere Analyse berücksichtigt.
2. Durch die Aktivierung der heuristischen Analyse wird "Re-Analyze" (Erneut analysieren) DEAKTIVIERT. Daher überprüft McAfee Advanced Threat Defense, ob bereits ein Analyseergebnis vorliegt. Wenn ja, wird dieses Ergebnis ohne weitere Analyse an den Manager weitergeleitet. Ist das Ergebnis nicht für denselben MD5-Hashwert verfügbar, folgt der nächste Analyseschritt.
3. Durch das Aktivieren der heuristischen Analyse wird der heuristische Filter ebenfalls AKTIVIERT, sodass McAfee Advanced Threat Defense die PDF-Dateistruktur auf Unregelmäßigkeiten untersucht. Wenn keine Unregelmäßigkeiten vorliegen, wird die Datei als sauber behandelt, und es wird keine weitere Analyse durchgeführt. Wenn heuristische Unregelmäßigkeiten vorliegen, wird die PDF-Datei gemäß dem entsprechenden Analyseprofil statisch und dynamisch analysiert.

Für Dateien, die nicht im PDF-Format vorliegen, wird nur die Option "Re-Analyze" (Erneut analysieren; siehe Schritt 2 oben) berücksichtigt.

Beispiel für das Deaktivieren der heuristischen Analyse: `set heuristic_analysis disable`

Wenn Sie dieses Beispiel ausführen, werden die folgenden Einstellungen angewendet:

1. Die Mindestdateigröße wird auf den Standardwert von 2.048 Byte festgelegt.
2. Durch das Deaktivieren der heuristischen Analyse wird "Re-Analyze" (Erneut analysieren) auf AKTIVIERT gesetzt, sodass McAfee Advanced Threat Defense alle unterstützten Dateien, die von Sensoren gesendet wurden, unabhängig davon überprüft, ob für diese Datei bereits Ergebnisse vorliegen oder nicht.
3. Durch das Deaktivieren der heuristischen Analyse wird der heuristische Filter ebenfalls DEAKTIVIERT, Daher werden PDF-Dateien von McAfee Advanced Threat Defense nicht auf heuristische Unregelmäßigkeiten untersucht. Die PDF-Dateien werden gemäß dem entsprechenden Analyseprofil statisch und dynamisch analysiert.

install msu

Mit diesem Befehl wird eine dieser beiden MSU-Dateien installiert:

- *amas-3.x.x.x.x.msu*
- *system-3.x.x.x.x.msu*

Syntax:

```
install msu
```

Parameter	Beschreibung
`<SWNAME>`	Der Name der MSU-Datei, die der Benutzer installieren möchte. Er lautet entweder "amas-3.x.x.x.x.msu" oder "system-3.x.x.x.x.msu".
`<RESET_DB>`	Von diesem Parameter werden nur zwei Werte (0/1) akzeptiert. "0" gibt an, dass bei Installation der MSU-Datei die Datenbank nicht zurückgesetzt wird. "1" gibt an, dass bei Installation der MSU-Datei die Datenbank zurückgesetzt wird.

Beispiel: `install msu amas-3.3.0.25.42303.msu 1`

lbstats

Zeigt die Statistik für den primären Knoten, den Sicherungsknoten und den sekundären Knoten in einem Lastenausgleichscluster an.

Dieser Befehl hat keine Parameter. Es erfolgt keine Ausgabe, wenn Advanced Threat Defense nicht Teil eines Clusters ist.

Syntax:

```
lbstats
```

Weitere Informationen finden Sie im Abschnitt Überwachen des Status eines Advanced Threat Defense-Clusters auf Seite 337.

list

Dieser Befehl listet alle dem Benutzer zur Verfügung stehenden CLI-Befehle auf.

Syntax: `list`

Dieser Befehl hat keine Parameter.

lowseveritystatus

Proben mit dem Schweregrad 1 und 2 werden von Advanced Threat Defense als Proben mit niedrigem Schweregrad und jene mit dem Schweregrad 3, 4 und 5 als bösartig behandelt. Wenn Sie die dynamische Analyse konfigurieren, wird der Wert der dynamischen Analyse für alle Proben standardmäßig im Übersichtsbericht angezeigt. Dieser Wert wirkt sich ebenfalls auf die Endbewertung der Probe aus. Bei Bedarf können Sie den Befehl `lowseveritystatus` verwenden, um dieses Verhalten zu ändern. Zum Beispiel zeigt Advanced Threat Defense den Wert der dynamischen Analyse für Proben mit niedrigem Schweregrad weder im Übersichtsbericht an, noch berücksichtigt sie diesen Wert bei der Berechnung der Endbewertung.

Der Befehl `lowseveritystatus` gilt nur für nicht portable ausführbare Proben wie Microsoft Word-Dokumente und PDF-Dateien.

Syntax: `lowseveritystatus <show><hide>`

Beispiel: `lowseveritystatus hide`

Parameter	Beschreibung
`show`	Dies ist das Standardverhalten. Wenn eine Probe dynamisch analysiert wird, zeigt Advanced Threat Defense den Wert der dynamischen Analyse im Bericht an. Dieser Wert wird ebenfalls bei der Berechnung der Endbewertung berücksichtigt.
`hide`	Angenommen, bei der Probe handelt es sich nicht um eine portable ausführbare Datei, für die eine dynamische Analyse ausgeführt wurde. Wenn Advanced Threat Defense erkennt, dass die Datei über einen niedrigen Schweregrad verfügt, wird der Wert der dynamischen Analyse nicht im Bericht (im Abschnitt **Analyseauswahl** unter **Sandbox** (Sandkasten)) angezeigt. Advanced Threat Defense berücksichtigt den Wert der dynamischen Analyse auch nicht bei der Berechnung der Endbewertung. Die Details zur dynamischen Analyse wie geöffnete und erstellte Dateien sind im Bericht enthalten. Der Befehl `lowseveritystatus hide` wirkt sich nur auf den im Bericht angezeigten Wert aus, nicht jedoch auf die auf der Seite **Analysis Results** (Analyseergebnisse) angezeigten Ergebnisse.

nslookup

Dieser Befehl zeigt das Abfrageergebnis für den nslookup-Befehl für den jeweiligen Domänennamen an. Sie können diesen Befehl verwenden, um zu überprüfen, ob McAfee Advanced Threat Defense nslookup-Abfragen korrekt durchführt.

Syntax: `nslookup <WORD>`

Parameter	Beschreibung
<WORT>	Dies ist der Domänenname, für den Sie die nslookup-Abfrage durchführen möchten.

Beispiel: `nslookup mcafee.com`

passwd

Dieser Befehl ändert das Kennwort des CLI-Benutzers (cliadmin). Das Kennwort muss zwischen 8 und 25 Zeichen umfassen und darf jedes alphanumerische Zeichen bzw. Symbol enthalten.

Vor dem Festlegen eines neuen Kennworts werden Sie aufgefordert, das aktuelle Kennwort einzugeben.

Syntax:

```
passwd
```

ping

Damit wird ein Ping-Befehl an einen Netzwerkhost oder Domänennamen gesendet. Sie können eine IPv4-Adresse zum Senden eines Ping-Befehls an Netzwerkhost und Domänennamen angeben, wenn Sie einen Ping-Befehl an einen Domänennamen senden möchten.

Syntax:

```
ping <A.B.C.D>
```

Parameter	Beschreibung
<A.B.C.D>	Dieser Befehl steht für eine 32-Bit-IP-Adresse eines Netzwerkhosts, dargestellt als vier durch Punkte getrennte 8-Bit-Nummern. Jede Nummer (A, B, C und D) ist eine 8-Bit-Nummer von 0–255.
<WORD>	Der Domänenname, an den Sie einen Ping-Befehl senden möchten.

quit

Dieser Befehl beendet CLI.

Dieser Befehl hat keine Parameter.

Syntax:

```
quit
```

reboot

Dieser Befehl startet die McAfee Advanced Threat Defense Appliance mit dem Image auf der aktuellen Festplatte neu. Sie müssen den Neustart bestätigen.

Syntax:

```
reboot
```

Parameter	Beschreibung
`reboot active`	Der Befehl startet die Appliance neu, mit der Softwareversion auf der aktiven Festplatte.
`reboot backup`	Der Befehl startet die Appliance neu, mit der Softwareversion auf der Sicherungsfestplatte.
`reboot vmcreator`	Dieser Befehl erstellt die in der McAfee Advanced Threat Defense-Web-Anwendung konfigurierten Analyse-VMs neu, während die Appliance neu gestartet wird.

resetuiadminpasswd

Verwenden Sie diesen Befehl zum Zurücksetzen des Kennworts für die *admin*-Benutzer der McAfee Advanced Threat Defense-Web-Anwendung. Wenn Sie diesen Befehl ausführen, wird das Kennwort auf den Standardwert zurückgesetzt, der *admin* lautet. Beachten Sie, dass die aktuell angemeldeten Sitzungen nicht betroffen sind. Eine Änderung des Kennworts betrifft nur neue Anmeldeversuche.

Syntax: `resetuiadminpasswd`

Drücken Sie "J" zum Bestätigen oder "N" zum Abbrechen.

resetusertimeout

Der Befehl ermöglicht Benutzern, sich bei der McAfee Advanced Threat Defense-Web-Anwendung anzumelden, ohne darauf zu warten, bis der Timer abläuft.

Syntax: `resetusertimeout <WORD>`

Parameter	Beschreibung
<WORD>	Der Benutzername für die McAfee Advanced Threat Defense-Web-Anwendung, für den Sie den Anmeldungszeitgeber entfernen möchten. Wenn die Aktion erfolgreich ist, wird die Nachricht *Reset done!* (Zurücksetzen ausgeführt) angezeigt.

Beispiel: `resetusertimeout admin`

restart network

Verwenden Sie diesen Befehl zum Neustarten des Netzwerks auf der McAfee Advanced Threat Defense. Starten Sie amas nach der Verwendung dieses Befehls neu.

Syntax: `restart network`

Dieser Befehl hat keine Parameter.

route add/delete network

Es stehen CLI-Befehle zum Hinzufügen und Entfernen statischer Routen zu McAfee Advanced Threat Defense zur Verfügung.

So fügen Sie einen Port hinzu:

```
route add network <Netzwerk-IP> netmask <Netzmaske> gateway <Gateway-IP> intfport
<Portnummer 1><Portnummer 2><Portnummer 3>
```

Beispiel: `route add network 1.1.1.0 netmask 255.255.255.0 gateway 1.1.1.1 intfport 1`

So löschen Sie einen Port:

```
route delete network <Netzwerk-IP> netmask <Netzmaske> gateway <Gateway-IP> intfport
<Portnummer 1><Portnummer 2><Portnummer 3>
```

Beispiel: `route delete network 1.1.1.0 netmask 255.255.255.0 gateway 1.1.1.1 intfport 1`

samplefilter

Dieser Befehl ist spezifisch für Network Security Platform-Sensoren. Verwenden Sie diesen Befehl, um zu verhindern, dass Sensoren nicht unterstützte Dateitypen zur Analyse an McAfee Advanced Threat Defense senden.

Syntax:

```
samplefilter <status><enable><disable>
```

Parameter	Beschreibung
status	zeigt an, ob die Probenfilterungsfunktion derzeit aktiviert oder deaktiviert ist. Sie ist standardmäßig aktiviert.
enable	setzt das Filtern der Proben auf "Aktiviert". Bei Aktivierung berücksichtigt McAfee Advanced Threat Defense nur die unterstützten Dateitypen von Network Security Platform für die Analyse. Eine Liste der unterstützten Dateien finden Sie unter Analysieren von Malware auf Seite 4. McAfee Advanced Threat Defense ignoriert alle anderen Dateitypen und informiert Network Security Platformdarüber, dass eine Probe einen nicht unterstützten Dateityp hat. Dadurch wird verhindert, dass Ressourcen für nicht unterstützte Dateitypen auf McAfee Advanced Threat Defense und Network Security Platform verwendet werden.
disable	setzt das Filtern der Proben auf "Deaktiviert". Bei Deaktivierung berücksichtigt McAfee Advanced Threat Defense alle von Network Security Platform eingesendeten Dateien, aber nur die unterstützten Dateitypen werden analysiert. Die übrigen werden auf den Seiten **Analysis Status** (Analysestatus) und **Analysis Results** (Analyseergebnisse) als nicht unterstützt gemeldet.

Beispiel:

```
samplefilter status
```

set appliance dns A.B.C.D E.F.G.H WORD

Mit diesem Befehl wird die bevorzugte und alternative DNS-Adresse von Advanced Threat Defense Appliance festgelegt.

Syntax:

```
set appliance dns A.B.C.D E.F.G.H WORD
```

Parameter	Beschreibung
<A.B.C.D>	Bevorzugte DNS-Adresse
<E.F.G.H>	Alternative DNS-Adresse
<WORD>	Domänenname der Appliance

Beispiel: `ATD-6000> set appliance dns 1.1.1.2 10.11.10.4 nai.com`

```
DNS setting had been configured
```

set intfport

Benutzen Sie diesen Befehl zum Aktivieren oder Deaktivieren desMcAfee Advanced Threat Defense-Schnittstellenanschlusses.

Syntax:

```
set intfport <1><2><3> <enable><disable>
```

Beispiel: `set intfport 1 enable`

set intfport auto

Dieser Befehl konfiguriert den Schnittstellenport für die automatische Aushandlung der Verbindung mit dem unmittelbarem Netzwerkgerät.

Syntax:

```
set intfport <1><2><3> auto
```

Beispiel:

```
set intfport 1 auto
```

set intfport ip

Dieser Befehl legt eine IP-Adresse für einen Schnittstellenport fest.

Syntax:

```
set intfport <1><2><3> auto
```

Beispiel:

```
set intfport 1 10.10.10.10 255.255.255.0
```

set intfport speed duplex

Dieser Befehl legt die Geschwindigkeits- und Duplex-Einstellungen für den spezifischen Schnittstellenanschluss fest.

Syntax:

```
set intfport <1><2><3> speed <10 | 100> duplex <half | full>
```

Parameter	Beschreibung
<1> <2> <3>	Geben Sie eine Schnittstellenanschluss-ID an, für die Sie Geschwindigkeit und Duplex einstellen möchten.
<10 | 100>	Legen Sie die damit die Geschwindigkeit für den Schnittstellenanschluss fest. Der Geschwindigkeitswert kann 10 oder 100 betragen.
<half | full>	Legen Sie damit die Duplex-Einstellung für den Schnittstellenanschluss fest. Setzen Sie den Wert auf "half" für Halb-Duplex und auf "full" für Voll-Duplex.

Beispiel:

```
set intfport 1 speed 100 duplex full
```

set malware-intfport

Mit diesem Befehl konfigurieren Sie den erforderlichen Port zur Weiterleitung des Internet-Datenverkehrs einer Analyse-VM.

Bevor Sie diesen Befehl ausführen, stellen Sie sicher, dass der erforderliche Port aktiviert und mit einer IP-Adresse konfiguriert ist.

Syntax: `set malware-intfport <1><2><3> gateway A.B.C.D`

Beispiel: `set malware-intfport 1 10.10.10.252`

Führen Sie `show intfport 1` aus und prüfen Sie die Einträge für `Malware Interface Port` und `Malware Gateway`.

McAfee Advanced Threat Defense verwendet den konfigurierten Port, um Analyse-VMs den Zugriff auf das Internet zu erlauben. Siehe Internetzugriff für Probedateien auf Seite 248.

set mgmtport auto

Dieser Befehl konfiguriert den Netzwerkanschluss für die automatische Aushandlung der Verbindung zwischen der McAfee Advanced Threat Defense-Appliance und dem unmittelbarem Netzwerkgerät.

Dieser Befehl hat keine Parameter.

Syntax:

```
set mgmtport auto
```

Standardwert:

Der Netzwerkanschluss ist automatisch auf **auto** (automatische Aushandlung) gesetzt.

set mgmtport speed and duplex

Dieser Befehl konfiguriert den Netzwerkanschluss so, dass er dieselbe Geschwindigkeit verwendet wie das Netzwerkgerät, das mit der McAfee Advanced Threat Defense-Appliance verbunden ist, und dass er im Voll- oder Halbduplexmodus betrieben wird.

Syntax:

```
set mgmtport <speed <10 | 100> duplex <full | half>>
```

Parameter	Beschreibung
<10|100>	Diese Zeichenfolge legt die Geschwindigkeit am Ethernet-Netzwerkanschluss fest. Der Wert für die Geschwindigkeit kann entweder 10 oder 100 Mbit/s betragen. Um die Geschwindigkeit auf 1000 Mbit/s zu setzen, benutzen Sie den Befehl `set mgmtport auto`.
<half|full>	Diese Zeichenfolge legt die Duplexeinstellung für den Ethernet-Netzwerkanschluss fest. Benutzen Sie den Wert `half` für Halbduplex und `full` für Vollduplex.

Standardwert:

Der Netzwerkanschluss ist automatisch auf **auto** (automatische Aushandlung) gesetzt.

set filesizes

Mit diesem Befehl können McAfee Advanced Threat Defense-Benutzer die minimale und maximale Dateigröße nach eigenem Bedarf ändern.

Syntax:

```
set filesizes <type number> <minimum size> <maximum size> <restart engine>
```

Parameter	Beschreibung
type number (Typnummer)	Typ der zur Analyse eingesendeten Datei.
minimum size (Mindestgröße)	Mindestgröße der Datei.
maximum size (Maximalgröße)	Maximale Dateigröße.
restart engine (Modul neu starten)	Verwendet den Wert 1 oder 0. 1 – AMAS-Dienst neu starten; dies ist für die NSP- und NGFW-Integration erforderlich. 0 – AMAS-Dienst läuft weiter; verwenden Sie diese Option, wenn die Einsendung über GUI/Rest-API erfolgt.

In der folgenden Tabelle werden die verschiedenen Dateitypen und ihre jeweilige **Typnummer**, **Mindestdateigröße** und **maximale Dateigröße** beschrieben:

Typnummer	Dateibeschreibung	Mindestgröße	Maximalgröße
1	Portierbare ausführbare EXE-, DLL- oder SYS-Datei (Windows)	1024	10000000
2	PDF-Dokumentdatei mit der Erweiterung .pdf	2048	25000000
3	Java-Klassendatei mit der Erweiterung .class	1024	5000000
4	Ältere Microsoft Office-Dateien mit der Erweiterung .doc, .ppt oder .xls	5120	10000000
5	Microsoft Rich Text Format-Datei mit der Erweiterung .rtf	1024	10000000
6	ZIP-Datei, APK-Datei oder neuere Microsoft Office-Datei mit der Erweiterung .docx, .pptx oder .xlsx	200	20000000
7	JPEG-Bilddatei	5120	1000000
8	PNG-Bilddatei	5120	1000000
9	GIF-Bild-/Bitmap-Datei	5120	1000000
10	Ausführbare Datei mit der Erweiterung .com (Microsoft DOS)	1024	5000000
11	Flash-Datei mit der Erweiterung .swf	1024	5000000
12	Komprimierte 7-Zip-Archivdatei mit der Erweiterung .7z	200	10000000
13	Komprimierte RAR-Archivdatei mit der Erweiterung .rar	200	10000000
14	Komprimierte Microsoft Cabinet-Archivdatei mit der Erweiterung .cab	200	10000000

Wenn ein Benutzer z. B. die Mindestdateigröße einer JPEG-Bilddatei in 300 Byte ändern möchte, wird durch den Befehl `set filesizes 7 300 1000000 0` die Mindestdateigröße für JPEG-Bilddateien in 300 Byte geändert.

set fips

Aktiviert oder deaktiviert den FIPS-Modus. Dieser Befehl hat keine Parameter. Starten Sie die McAfee Advanced Threat Defense Appliance neu, wenn Sie den FIPS-Modus aktivieren oder deaktivieren.

Syntax: `set fips <enable> <disable>`

set ftp

Wenn Sie Dateien zur Analyse mit einem FTP-Client hochladen oder wenn Sie eine VMDK-Datei in McAfee Advanced Threat Defense importieren, um eine Analyse-VM zu erstellen, verwenden Sie SFTP, da FTP standardmäßig nicht unterstützt wird. Sollten Sie jedoch FTP für diese Aufgaben bevorzugen, können Sie FTP aktivieren.

Syntax: `set ftp <enable><disable>`

In der Standardeinstellung ist FTP deaktiviert.

Beispiel: `set ftp enable`

Siehe auch: show ftp auf Seite 368.

set heuristic_analysis

Siehe heuristic_analysis auf Seite 354.

set appliance gateway

Dieser Befehl legt die IPv4-Adresse des Gateways für die McAfee Advanced Threat Defense-Appliance fest.

Syntax:

```
set appliance gateway <A.B.C.D>
```

Parameter	Beschreibung
<A.B.C.D>	Eine 32-Bit-Adresse, die als vier 8-Bit-Zahlen geschrieben ist; die vier Zahlen sind durch Punkte voneinander getrennt. A, B, C oder D stehen für eine 8-Bit-Zahl zwischen 0 und 255.

Beispiel:

```
set appliance gateway 192.34.2.8
```

set appliance ip

Dieser Befehl legt die IPv4-Adresse und die Subnetzmaske für die McAfee Advanced Threat Defense-Appliance fest. Damit die Änderung der IP-Adresse aktiviert wird, ist ein Neustart erforderlich. Im Abschnitt zum Befehl `reboot` erhalten Sie Anweisungen zum Neustarten der McAfee Advanced Threat Defense-Appliance.

Syntax:

```
set appliance ip <A.B.C.D E.F.G.H>
```

Parameter	Beschreibung
<A.B.C.D E.F.G.H>	Diese Zeichenfolge gibt die IPv4-Adresse gefolgt von einer Netzmaske an. Bei der Netzmaske wird die Host-ID-Adresse aus der IP-Adresse entfernt, sodass nur die Netzwerk-ID übrig bleibt. Jede Netzmaske besteht aus Binär-Einsern (Dezimal-255) zur Darstellung der Netzwerk-ID und aus Binär-Nullen (Dezimal-Nullen), dank der die Host-ID der IP-Adresse beibehalten wird. (Beispiel: Die standardmäßige Netzmaskenkeinstellung für eine Adresse der Klasse C lautet 255.255.255.0).

Beispiel:

```
set appliance ip 192.34.2.8 255.255.0.0
```

set appliance name

Dieser Befehl legt den Namen der McAfee Advanced Threat Defense-Appliance fest. Der Name dient zur Identifizierung der McAfee Advanced Threat Defense-Appliance, wenn Sie diese in Network Security Platform integrieren.

Syntax:

```
set appliance name <WORD>
```

Parameter	Beschreibung
<WORD>	Gibt eine Folge von bis zu 25 Zeichen an, bei denen die Groß- und Kleinschreibung beachtet werden muss. Die Zeichenfolge kann Bindestriche, Unterstriche und Punkte enthalten und muss mit einem Buchstaben beginnen.

Beispiel:

```
set appliance name SanJose_MATD1
```

set uilog

Verwenden Sie diesen Befehl, um den Umfang der zu protokollierenden Informationen zum UI-Zugriff festzulegen. Es sind Stufen zwischen 1 und 7 möglich.

Syntax:

```
set uilog<seconds>
```

Parameter	Beschreibung
<numeric>	Legt den Umfang der zu protokollierenden Informationen zum UI-Zugriff fest.

```
ATD-6000> set uilog 5 new log level is 5
```

set ui-timeout

Dieser Befehl legt fest, wie viele Minuten Inaktivität verstreichen können, bevor es bei der Verbindung zur McAfee Advanced Threat Defense-Web-Anwendung zu einer Zeitüberschreitung kommt.

Syntax:

```
set ui-timeout <60 - 86400>
```

Parameter	Beschreibung
<60 - 86400>	Sie können für die Zeitüberschreitung eine Dauer von 60 bis 86.400 Sekunden einstellen.

Beispiel: `set ui-timeout 600`

Standardwert: 15 Minuten

set waittime

Verwenden Sie diesen Befehl, um die maximale Wartezeit für die Analyse der Proben von McAfee Email Gateway zu konfigurieren. Liegt die durchschnittliche Analysezeit der Proben in Advanced Threat Defense über der durch diesen Befehl festgelegten Schwelle, werden die von McAfee Email Gateway eingesendeten Proben abgewiesen.

Syntax:

```
set waittime <seconds>
```

Parameter	Beschreibung
<seconds>	Legt die Anzahl an Sekunden der maximalen Wartezeit fest.

Beispiel

```
set waittime 20
```

set whitelist

Verwenden Sie diesen Befehl, um die Überprüfung der Whitelist durch McAfee Advanced Threat Defense zu konfigurieren. Dieser ist standardmäßig aktiviert.

Syntax: `set whitelist <enable><disable>`

Beispiel: `set whitelist enable`

show

Mit diesem Befehl werden die aktuellen Konfigurationseinstellungen der McAfee Advanced Threat Defense Appliance angezeigt.

Dieser Befehl hat keine Parameter.

Syntax:

```
show
```

Zu den Informationen, die durch den Befehl `show` angezeigt werden, zählen:

[Sensor Info]

- Systemname
- Datum
- Systembetriebszeit
- Systemtyp
- Seriennummer
- Softwareversion
- Aktive Version
- Sicherungsversion
- MGMT-Ethernet-Anschluss

[Sensor Network Config]

- IP-Adresse
- Netzwerkmaske
- Standard-Gateway
- DNS-Adresse

show epo-stats nsp

Dieser Befehl zeigt die Anzahl der an McAfee ePOgesendeten Anfragen, die Anzahl der von McAfee ePOerhaltenen Antworten sowie die Anzahl von fehlgeschlagenen Anfragen an.

Syntax: `show epo-stats nsp`

Dieser Befehl hat keine Parameter.

show filesizes

Mit diesem Befehl werden alle von McAfee Advanced Threat Defense unterstützten Dateitypen mit Details wie der Typnummer, der minimalen und maximalen Dateigröße (in Byte) sowie einer Kurzbeschreibung angezeigt.

Dieser Befehl hat keine Parameter.

Syntax:

```
show filesizes
```

Im Folgenden werden die Informationen, die durch den Befehl `show filesizes` angezeigt werden, dargestellt:

Typnummer	Dateibeschreibung	Mindestgröße	Maximalgröße
1	Portierbare ausführbare EXE-, DLL- oder SYS-Datei (Windows)	1024	10000000
2	PDF-Dokumentdatei mit der Erweiterung .pdf	2048	25000000
3	Java-Klassendatei mit der Erweiterung .class	1024	5000000
4	Ältere Microsoft Office-Dateien mit der Erweiterung .doc, .ppt oder .xls	5120	10000000
5	Microsoft Rich Text Format-Datei mit der Erweiterung .rtf	1024	10000000
6	ZIP-Datei, APK-Datei oder neuere Microsoft Office-Datei mit der Erweiterung .docx, .pptx oder .xlsx	200	20000000
7	JPEG-Bilddatei	5120	1000000
8	PNG-Bilddatei	5120	1000000
9	GIF-Bild-/Bitmap-Datei	5120	1000000
10	Ausführbare Datei mit der Erweiterung .com (Microsoft DOS)	1024	5000000
11	Flash-Datei mit der Erweiterung .swf	1024	5000000
12	Komprimierte 7-Zip-Archivdatei mit der Erweiterung .7z	200	10000000
13	Komprimierte RAR-Archivdatei mit der Erweiterung .rar	200	10000000
14	Komprimierte Microsoft Cabinet-Archivdatei mit der Erweiterung .cab	200	10000000

show fips

Zeigt an, ob FIPS derzeit aktiviert oder deaktiviert ist. Dieser Befehl hat keine Parameter.

Syntax: `show fips`

show ftp

Verwenden Sie diesen Befehl, um zu erfahren, ob FTP derzeit aktiviert oder deaktiviert ist. In der Standardeinstellung ist FTP deaktiviert.

Syntax: `show ftp`

Siehe auch: set ftp auf Seite 364.

show history

Dieser Befehl ruft eine Liste der in der Sitzung benutzten CLI-Befehle auf.

Syntax: `show history`

Dieser Befehl hat keine Parameter.

show heuristic_analysis

Siehe heuristic_analysis auf Seite 354.

show intfport

Dieser Befehl zeigt den Status des angegebenen Schnittstellen- oder Verwaltungsports von McAfee Advanced Threat Defense an.

Syntax: `show intfport <mgmt><1><2><3>`

Zu den Informationen, die durch den Befehl `show intfport` angezeigt werden, zählen:

- Angabe, ob der Administrationsstatus aktiviert oder deaktiviert ist
- Verknüpfungsstatus des Ports
- Geschwindigkeit des Ports
- Angabe, ob der Port auf Halb- oder Vollduplex eingestellt ist
- Insgesamt erhaltene Pakete
- Insgesamt gesendete Pakete
- Insgesamt erhaltene CRC-Fehler
- Insgesamt erhaltene andere Fehler
- Insgesamt gesendete CRC-Fehler
- Insgesamt gesendete andere Fehler
- IP-Adresse des Ports
- MAC-Adresse des Ports
- Angabe, ob der Port verwendet wird, um Analyse-VMs den Zugriff auf das Internet zu erlauben
- Bei Konfiguration mit Bereitstellung von Internetzugriff für Analyse-VMs: entsprechendes Gateway für diesen Datenverkehr

show msu

Mit diesem Befehl werden alle über SFTP auf Advanced Threat Defense kopierten MSU-Dateien angezeigt.

Syntax: `show msu`

show nsp scandetails

Dieser Befehl zeigt die Dateiscan-Details zu den integrierten IPS-Sensoren an.

Syntax: `show nsp scandetails <Sensor-IP-Adresse>`

Wenn Sie keine IP-Adresse für den Sensor angeben, werden die Details für alle in der McAfee Advanced Threat Defense-Appliance integrierten Sensoren angezeigt.

Zu den mittels `show nsp scandetails`-Befehl angezeigten Informationen zählen:

- IP-Adresse des IPS-Sensors
- Gesamtanzahl der vom Sensor empfangenen Pakete
- Gesamtanzahl der an den Sensor gesendeten Pakete
- Zeitstempel des letzen an den Sensor gesendeten und von ihm empfangenen Pakets
- Zur Kommunikation mit dem Sensor benutzte Verschlüsselungsmethode
- Null-Anzahl bei Sitzungshandles
- Anzahl der internen Fehler
- Anzahl der vom Sensor empfangenen unbekannten Befehle
- Null-Dateizeichenfolgen
- Null-Dateidaten
- Anzahl der unbekannten Dateien
- Anzahl der irregulären Pakete
- Anzahl von MD5-Konflikten zwischen den vom Sensor gesendeten und von McAfee Advanced Threat Defense empfangenen Inhalten
- Fehleranzahl bei der Speicherzuteilung
- Zeitüberschreitung bei der Dateiübertragung
- Anzahl der neuen Dateien
- Fehleranzahl bei der Shared Memory-Zuteilung
- Anzahl der gesendeten statischen Analyseanworten
- Anzahl der gesendeten dynamischen Analyseanworten
- Anzahl der empfangenen Scan-Anfragen
- MD5 der letzten vom Sensor gestreamten Datei

show route

Dieser Befehl wird zum Anzeigen von Routen benutzt, die Sie mithilfe des `route add`-Befehls und in der IP-Routingtabelle erstellt haben.

Syntax:

```
show route
```

In der nachstehenden Tabelle sehen Sie Details zu einer Beispielausgabe des Befehls.

Tabelle 9-2 System-IP-Routingtabelle

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
10.10.10.0	0.0.0.0	255.255.255.0	U	0	0	0	mgmt
11.11.11.0	0.0.0.0	255.255.255.0	U	0	0	0	mgmt
12.12.0.0	0.0.0.0	255.255.0.0	U	0	0	0	mgmt

Tabelle 9-2 System-IP-Routingtabelle *(Fortsetzung)*

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
13.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	mgmt
0.0.0.0	10.10.10.253	0.0.0.0	UG	0	0	0	mgmt

show ui-timeout

Mit diesem Befehl wird das Zeitlimit des McAfee Advanced Threat Defense-Web-Anwendungsclients in Sekunden angezeigt.

Syntax: `show ui-timeout`

Ausgabebeispiel: `Current timeout value: 600`

show uilog

Verwenden Sie diesen Befehl, um die aktuelle Stufe für uilog zu prüfen.

Dieser Befehl hat keine Parameter.

Syntax:

```
show uilog
```

Im Folgenden werden die Informationen, die durch den Befehl `show uilog` angezeigt werden, dargestellt:

```
ATD-6000> show uilog
Current log level is 7
```

show version

Zeigt die Zebra-Version von McAfee Advanced Threat Defense an.

Dieser Befehl hat keine Parameter.

Syntax:

```
show version
```

Im Folgenden werden die Informationen, die durch den Befehl `show uilog` angezeigt werden, dargestellt:

```
Zebra 0.95a ().
Copyright 1996-2004, Kunihiro Ishiguro.
ATD-3000>
```

show waittime

Mit diesem Befehl wird der für McAfee Email Gateway eingestellte Schwellenwert für die Wartezeit angezeigt.

Syntax: `show waittime`

Ausgabebeispiel: `Current MEG wait time threshold=780 seconds`

shutdown

Dieser Befehl hält die McAfee Advanced Threat Defense-Appliance an, damit Sie sie herunterfahren können. Nach zirka einer Minute können Sie die McAfee Advanced Threat Defense-Appliance **manuell** ausschalten und beide Netzteile ausstecken. Die McAfee Advanced Threat Defense-Appliance schaltet sich nicht automatisch aus. Sie müssen das Ausschalten bestätigen.

Dieser Befehl hat keine Parameter.

Syntax:

```
shutdown
```

status

Der Befehl zeigt den Systemstatus von McAfee Advanced Threat Defense an, beispielsweise den Zustand und die Anzahl von Dateien, die an verschiedene Module gesendet wurden.

Dieser Befehl hat keine Parameter.

Syntax: `status`

Ausgabebeispiel:

```
System Health Status : good

Sample files received count: 300

Sample files submitted count: 300

GTI Scanner files submitted count: 50

GAM Scanner files submitted count: 100

MAV Scanner files submitted count: 200

Sandbox files submitted count: 25

Sandbox files finished count: 25

Sample files finished count: 300

Sample files error count: 0
```

terminal

Mit diesem Befehl wird die Anzahl von Zeilen zur Anzeige auf dem Bildschirm der McAfee Advanced Threat Defense festgelegt.

Syntax:

```
terminal <length>¦no
```

Parameter	Beschreibung
<length>	Legt die Anzahl von Zeilen zur Anzeige auf dem Bildschirm fest. Der Wert reicht von 0 bis 512.
no	Negiert den vorherigen Befehl oder legt den Standardwert fest.

update_avdat

McAfee Advanced Threat Defense aktualisiert standardmäßig alle 90 Minuten die DAT-Dateien für McAfee Gateway Anti-Malware Engine und McAfee Anti-Malware Engine. Verwenden Sie den Befehl `update_avdat`, um diese Dateien umgehend zu aktualisieren.

Dieser Befehl hat keine Parameter.

Syntax: `update_avdat`

Vmlist

Zeigt eine Liste aller auf der McAfee Advanced Threat Defense konfigurierten VMs an

Syntax: `vmlist`

watchdog

Der Watchdog-Vorgang startet die McAfee Advanced Threat Defense-Appliance neu, wenn ein nicht behebbarer Fehler erkannt wird.

Syntax:

`watchdog <on | off | status>`

Parameter	Beschreibung
<on>	Damit aktivieren Sie die Watchdog-Funktion.
<off>	Damit deaktivieren Sie die Watchdog-Funktion. Verwenden Sie diesen Befehl, wenn die Appliance aufgrund wiederholter Systemfehler immer wieder neu startet.
<status>	Dies zeigt den Status des Watchdog-Vorgangs an.

set malware-intfport mgmt

Standardmäßig erfolgt der Internetzugriff für Analyse-VMs über den Verwaltungsport von McAfee Advanced Threat Defense (ETH-0). Verwenden Sie diesen Befehl, wenn Sie einen anderen Port zum Routen des Internet-Datenverkehrs konfiguriert haben und zum Verwaltungsport zurückkehren möchten.

Syntax: `set malware-intfport mgmt`

Führen Sie `show intfport mgmt` aus und prüfen Sie die Einträge für `Malware Interface Port` und `Malware Gateway`.

McAfee Advanced Threat Defense verwendet den Verwaltungsport, um Analyse-VMs den Zugriff auf das Internet zu erlauben. Siehe Internetzugriff für Probedateien auf Seite 248.

whitelist

Verwenden Sie folgende Befehle, um die Whitelist von McAfee Advanced Threat Defense zu verwalten.

Syntax:

- Verwenden Sie `whitelist add <md5>`, um der Whitelist einen MD5-Wert hinzuzufügen.

  Beispiel: `whitelist add 254A40A56A6E68636E1465AF7C42B71F`

- Verwenden Sie `whitelist delete <md5>`, um einen MD5-Wert von der Whitelist zu löschen.

  Beispiel: `whitelist delete 254A40A56A6E28836E1465AF7C42B71F`

- Verwenden Sie `whitelist query <md5>`, um zu überprüfen, ob ein MD5-Wert in der Whitelist vorhanden ist.

  Beispiel: `whitelist query 254A40A56A6E28636E1465AF7C42B71F`

- Verwenden Sie `whiteliststatus`, um zu überprüfen, ob der Whitelist-Status derzeit aktiviert ist.

Index

A

Aktive Festplatte 347
Analyse-VM 243
    Erstellen 71
Analyseergebnisse
    Anzeigen 294
    Cluster 342
Analyseprofil 243
    Änderung 256
    Anzeigen 252
    Hinzufügen 253
    Löschen 256
    Verwaltung 251
Analysestatus
    Cluster 341
    Überwachen 290
Anti-Malware Engine 243
Anzeigen der Analyseergebnisse 294

B

Begriffe 243
Benutzer 243
Benutzerdefinierte YARA-Regeln 271
Berichte
    Analyseübersicht 297
    Betroffene Dateien 304
    Disassembly-Ergebnisse 304
    Logisches Pfaddiagramm 305

C

CLI-Anmeldung 347
CLI-Befehle
    Liste 348
    Obligatorische Befehle 347
    Syntax 346
    Vorgehensweise 345
CLI-Befehlsausgabe
    Auto-Vervollständigung 346
    Konsole 345
    SSH 346

D

Dashboard 312
Datenbank
    Sichern und Wiederherstellen 61
Datum und Uhrzeit 267, 274, 277, 278
Diagnosedateien 59
Disk-A 347
Disk-B 347
Dokumentation
    Produktspezifisch, suchen 10
    Typografische Konventionen und Symbole 9
    Zielgruppe dieses Handbuchs 9
dynamische Analyse 243

E

ePO-Server-Integration 256
ePO-Server-Konfiguration 258, 260
Exportieren von Protokollen 59

F

Fehlerbehebung 58

G

Gateway Anti-Malware Engine 243

H

Handbuch, Informationen 9
Hochladen von Dateien
    manuell 280
    SFTP 286
    Web-Anwendung 280
Hochladen von Proben
    manuell 280
    SFTP 286
    Web-Anwendung 280
Hochladen von URLs
    interaktiver Benutzermodus 281
    manuell 288
    Web-Anwendung 288

I

interaktiver Benutzermodus 281

Internet-Proxy-Server 261–263
Internetzugriff 248

J

JSON 297

K

Konfiguration der Malware-Analyse
    Grundlegende Schritte 247
    Überblick 243
Konfiguration von DNS-Einstellungen 264, 267
Konventionen und Symbole in diesem Handbuch 9

L

lokale Blacklist 243
lokale Whitelist 243

M

Malware-Analyse 279
    Prozessablauf 248, 279, 287
McAfee Advanced Threat Defense
    Benutzerverwaltung 37, 261
    Bereitstellungsoptionen 14
    Beschreibung der Lösung 12
    Dashboard 312
    Festplatten 347
    Leistungsmonitore 317
    Leistungsüberwachung 44
    Sichern und Wiederherstellen 61
    Software-Import 45, 51, 53
    Upgrade 45, 51, 53
    Vorteile 17
    Zugreifen auf die Web-Anwendung 36
McAfee Advanced Threat Defense Appliance
    Einrichten 19, 27
    Hardware-Spezifikationen 25
    Wichtige Informationen 20
McAfee ServicePortal, Zugriff 10
Monitore
    Malware-Analyse 313
    VM Creation Status 317

N

Netzwerksimulator 248

O

OpenIOC 297

P

Probenanalyse 279
Protokolldateien 59
Prozessablauf 256

R

Real Internet-Modus 248

S

Sensor-Anmeldung; SSH 346
ServicePortal, Quellen für Produktinformationen 10
Sichern und Wiederherstellen 61
Sicherungsfestplatte 347
Simulationsmodus 248
statische Analyse 243
STIX 297
Supportpaket 59
Systemanforderungen
    Client 35

T

Technischer Support, Produktdokumentation finden 10

U

Überblick 11
User API-Protokoll 310

V

verwendete Portnummern 27
VM-Erstellungsprotokoll 241
VM-Profil 243
    Anzeigen 234
    Bearbeiten 240
    Erstellen 234
    Hinzufügen 234
    Löschen 241
    Verwaltung 233
VMDK-Datei
    Image-Konvertierung 230
    Importieren 230

W

Warnungen 21

X

X-Mode 281
XML 297
XMode 281

Y

YARA-Regeln 271